File 348:EUROPEAN PATENTS 1978-2004/Feb W05
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040304,UT=20040226
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	7866	TTL OR TIME(3W)LIVE
S2	30965	TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S3	1068	IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5
S4	1784018	VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALID? OR CHECK?-?? ? OR CHEQU??? ? OR EXAMIN? OR TEST OR TESTS OR TESTED OR T-ESTING? OR EVALUAT? OR CONFIRM?
S5	25689	AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CRO-SSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQ?
S6	958505	SCREEN? OR INSPECT? OR DETERMIN? OR ASSESS? OR MONITOR?
S7	186220	S4:S6(3N)(PACKET OR PACKETS OR CONTENT OR CONTENTS OR ECON-TENT? ? OR MESSAGE OR MESSAGES OR DATA OR FILE OR FILES OR OB-JECT OR OBJECTS)
S8	24	S1(25N)S2:S3
S9	23	S8 NOT (DIODE? ? OR WIND()TUNNEL?)

9/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01510491
Method of establishing a secure tunnel through a proxy server between a user device and a secure server
Verfahren zur Herstellung eines sicheren Tunnels durch einen Proxyserver zwischen einem Benutzergerat und einem sicheren Server
Methode pour construire un tunnel securise a travers un serveur proxy entre un dispositif d'utilisateur et un serveur securise
PATENT ASSIGNEE:
Openwave Systems Inc., (3397261), 1400 Seaport Boulevard, Redwood City, CA 94063, (US), (Applicant designated States: all)
INVENTOR:
King, Peter F., 438 Magellan Avenue, Half Moon Bay, CA 94019, (US)
LEGAL REPRESENTATIVE:
Jehle, Volker Armin (95141), Bosch, Graf von Stosch, Jehle, Patentanwalte, Theatinerstrasse 8, 80333 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1263186 A2 021204 (Basic)
APPLICATION (CC, No, Date): EP 2002011758 020527;
PRIORITY (CC, No, Date): US 872997 010531
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-029/06

ABSTRACT EP 1263186 A2
A method and apparatus for establishing a secure tunnel through a proxy between a user device and a secure server on a network are described. The method comprises storing information retrievable by the proxy server, in the event of the user device sending a request to the proxy server to access the secure server during a current session with the proxy server. The information indicates that the user device wishes to access the secure server. Thereafter, the current session between the user device and the proxy server is terminated. A tunnel is set through the proxy server between the user device and the secure server (via a trusted domain proxy/firewall) in the event of the user device sending a further request to the proxy server to access the secure server.
ABSTRACT WORD COUNT: 131
NOTE:
Figure number on first page: 4

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 021204 A2 Published application without search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200249	1570
SPEC A	(English)	200249	3163
Total word count - document A			4733
Total word count - document B			0
Total word count - documents A + B			4733

...SPECIFICATION 114. If a positive match is made, then at 314 proxy server 106 goes into **tunnel** mode with a **time** -to- **live** delay. In other words, proxy server 106 will continue to operate in **tunnel** mode for a predetermined period of time, beyond which it will terminate the tunnel. If...

...to perform standard proxy services in a nontunnel mode. At 316, proxy server 106 will **tunnel** data between mobile telephone 110 and secure server 114 (via the trusted domain proxy/firewall 112) until the **time** to- **live** -delay has been reached, or it is determined, at 318, that the **tunnel** is to be terminated. Proxy server 106 is able to determine that the tunnel has...

...CLAIMS receipt of the further request.

10. The method of claim 1 further comprising establishing a **time** -to- **live** default for the **tunnel** , beyond which time the **tunnel** is terminated.
11. The method of claim 1 which comprises terminating the **tunnel** upon the occurrence of a predetermined event.
12. The method of claim 11 wherein the...

...machine readable program storage medium of claim 14, wherein the method further comprises establishing a **time** -to- **live** default for the **tunnel** , beyond which time the **tunnel** is terminated.

24. The machine readable program storage medium of claim 14, wherein the method...The proxy server of claim 28, wherein the code further comprises instructions to establish a **time** -to- **live** default for the **tunnel** , beyond which time the **tunnel** is terminated.
37. The proxy server of claim 1, wherein the code further comprises instructions...

9/5,K/2 (Item 2 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01319208

Data processing device, system and method using a state transition table
Datenverarbeitungsvorrichtung, -system und -verfahrung benutzend eine Zustandstransitiontabelle
Appareil, systeme et methode de traitement de donnees utilisant une table de transition entre etats

PATENT ASSIGNEE:
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States: all)

INVENTOR:
Jinzaki, Akira, c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)

LEGAL REPRESENTATIVE:
Stebbing, Timothy Charles et al (59641), Haseltine Lake & Co., Imperial House, 15-19 Kingsway, London WC2B 6UD, (GB)

PATENT (CC, No, Kind, Date): EP 1126367 A1 010822 (Basic)
APPLICATION (CC, No, Date): EP 2001301333 010215;
PRIORITY (CC, No, Date): JP 200036874 000215
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G06F-009/00

ABSTRACT EP 1126367 A1

A data processing device that performs processes for general-purpose

data, such as a stream data process, etc., at high speed, and can flexibly change in function according to the circumstances, and comprises an input converting unit (2) obtaining memory search data from input data; a memory searching unit (3) searching, based on the memory search data, a state transition table (4) storing as an entry a state word which designates a preset process, and reading the state word corresponding to a process performed for the input data; an arithmetic operation unit (5) determining the process performed for the input data based on contents of the state word read by said memory searching unit (3), and performing the process.

ABSTRACT WORD COUNT: 119

NOTE:
Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 010822 A1 Published application with search report
Examination: 011024 A1 Date of request for examination: 20010828
Examination: 011219 A1 Date of dispatch of the first examination report: 20011105

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200134	1917
SPEC A	(English)	200134	14578
Total word count - document A			16495
Total word count - document B			0
Total word count - documents A + B			16495

...SPECIFICATION be measured, at least 1 is subtracted from the TTL value. When a packet whose **TTL** value is 0 is detected in a partway IP module, this packet is discarded.

As an example of more complicated packet labeling, **IPsec** (Security Architecture for the Internet Protocol) exists. By way of example, with the ESP (Encapsulated...

9/5,K/3 (Item 3 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01261498

Packet network interfacing
Datennetzschnittstelle
Interface pour un reseau de donnees

PATENT ASSIGNEE:
BRITISH TELECOMMUNICATIONS public limited company, (846100), 81 Newgate Street, London EC1A 7AJ, (GB), (Applicant designated States: all)

INVENTOR:
The designation of the inventor has not yet been filed

LEGAL REPRESENTATIVE:
Semos, Robert Ernest Vickers et al (43051), BT Group Legal Services, Intellectual Property Department, 8th Floor, Holborn Centre 120 Holborn , London EC1N 2TE, (GB)

PATENT (CC, No, Kind, Date): EP 1087575 A1 010328 (Basic)
APPLICATION (CC, No, Date): EP 99307550 990924;
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-012/46

ABSTRACT EP 1087575 A1

A method of establishing a tunnel across an IPv4 domain for the transport of packets from a source host on one IPv6 domain to a destination host on another IPv6 domain, there being respective interfaces between the IPv4 domain and the IPv6 domains. The source host sends a normal IPv6 address request to its local DNS server, which relays it to an IPv6 name server in the other IPv6 domain. The response message, containing the true IPv6 address of the destination is received at the

remote interface, which appends to the resulting protocol converted DNS response message a first additional record containing the true IPv6 address, and a second additional record containing the IPv4 address of that interface. Upon receipt at the near interface, the additional records are stripped off, their contents stored in an entry of a table, and the true IPv6 address written into the address record of the resulting IPv6 DNS response message. When the near interface receives a packet from an IPv6 host, it checks whether the destination address matches an entry of its table, and if so sends the packet to the encapsulator together with the IPv4 address of the remote interface. The remote interface extracts the source address and the address of the encapsulating interface and stores these in an entry in its corresponding table for use in encapsulating return packets to the source. If, however, the destination address is recognised as being of IPv4-compatible or IPv4-mapped format, the packet is sent to a protocol converter.

ABSTRACT WORD COUNT: 253

NOTE:

Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application: 010328 A1 Published application with search report

Withdrawal: 011205 A1 Date application deemed withdrawn: 20010125

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200113	992
SPEC A	(English)	200113	6284
Total word count - document A			7276
Total word count - document B			0
Total word count - documents A + B			7276

...SPECIFICATION deleted at midnight, when the day changes, or the address can be stored with a " **time** to **live** " value which is the start value of a count down timer. Similarly, the border router 16A deletes the entry in its IPv6/ **tunnel** endpoint table 76A after a short time. By preventing permanent storage of the address of...

...CLAIMS stored retrieved content, and rendering that stored retrieved content unuseable upon the expiry of the **time** to **live** .

8. A method as claimed in claim 7, wherein the rendering step deletes the stored retrieved content.

9. A method of establishing a **tunnel** from a first interface between a first network and a second network to a second...

9/5,K/4 (Item 4 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

00979126

Method and apparatus for client-host communication over a computer network

Verfahren und Vorrichtung zur Klient-Server-Kommunikation uber ein Rechnernetz

Procede et dispositif pour la communication de client-serveur par un reseau d'ordinateurs

PATENT ASSIGNEE:

SUN MICROSYSTEMS, INC., (1392730), 2550 Garcia Avenue, Mountain View, CA 94043, (US), (Applicant designated States: all)

INVENTOR:

Aziz, Ashar, House 143, Street 43, F-10/4, Islamabad, (PK)

Markson, Thomas, 30 Mounds Road, Apt. 206, San Mateo, CA 94402, (US)

LEGAL REPRESENTATIVE:

Fiener, Josef (70561), Patentanwalte Kahler, Kack, Fiener et col., P.O. Box 12 49, 87712 Mindelheim, (DE)

PATENT (CC, No, Kind, Date): EP 887979 A2 981230 (Basic)
EP 887979 A3 010214

APPLICATION (CC, No, Date): EP 98111746 980625;

PRIORITY (CC, No, Date): US 883676 970627

DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-029/06; H04L-012/22; H04L-009/32; H04L-029/12

ABSTRACT EP 887979 A2
According to the invention, a method and apparatus are provided for dynamically configuring authorized clients with the address of a protected host and the key and address of an intermediate device (e.g., encrypting firewall, encrypting router, secure gateway) which is protecting a number of hosts on a private network located topologically behind that intermediate device. The registered name server for a domain is configured to return a new resource record type, herein called an SX record, in response to requests for information needed for secure communications with protected hosts in that domain. The resolver on (or otherwise associated with) the authorized client is configured to use the data in the SX record to dynamically update the information used by the client to handle secure communications.
ABSTRACT WORD COUNT: 126
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Change:	010214	A2	International Patent Classification changed: 20001223
Application:	981230	A2	Published application (A1with Search Report ;A2without Search Report)
Withdrawal:	030702	A2	Date application deemed withdrawn: 20021231
Examination:	010829	A2	Date of request for examination: 20010702
Search Report:	010214	A3	Separate publication of the search report
Change:	990210	A2	Title of invention (German) (change)
Change:	990728	A2	Inventor (change)

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9853	2399
SPEC A	(English)	9853	7796
Total word count - document A			10195
Total word count - document B			0
Total word count - documents A + B			10195

...SPECIFICATION can easily accommodate any changes to the content or location of the information in a **tunnel** map.
Those skilled in the art know that resource records contain a **time** -to- **live** (**TTL**) field that indicates how long the record's information can be relied upon. The **TTL** field in the SX record could be used to determine the life of the **tunnel** map entries derived from that record. However, other methods, such as reinitializing the tunnel map...

9/5,K/7 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01089554 **Image available**
METHOD AND APPARATUS FOR RECEIVABILITY TEST AND REACHABILITY TEST OF EXPLICIT MULTICAST
PROCEDE ET APPAREIL DE TEST DE RECEVABILITE ET DE TEST D'ACCESSIBILITE MULTIDESTINATION EXPLICITE
Patent Applicant/Assignee:
KTFREETEL CO LTD, 890-20 Daechi-dong, Gangnam-gu, 135-280 Seoul, KR, KR (Residence), KR (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
LEE Ji-Woong, #501 1357-63 Seocho-dong, Seocho-gu, 137-070 Seoul, KR, KR (Residence), KR (Nationality), (Designated only for: US)
Legal Representative:
LEE Kyeong-Ran (agent), 502 BYC Bldg., 648-1 Yeoksam 1-dong, Kangnam-ku, 135-081 Seoul, KR,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200412394 A1 20040205 (WO 0412394)
Application: WO 2002KR1448 20020731 (PCT/WO KR02001448)
Priority Application: WO 2002KR1448 20020731
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/26
Publication Language: English
Filing Language: Korean
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4012

English Abstract
The present invention relates to method and apparatus for receivability test and reachability test of explicit multicast packet. The xcast receivability test according to the present invention comprises the steps of: at a sender end, sending a receivability probe packet to a receiver end; at the receiver end, receiving the receivability probe packet; generating an ICMP error message-Destination Unreachable; sending the ICMP error message-Destination Unreachable to sender end; at the sender end, receiving the ICMP error message-Destination Unreachable; and analyzing the ICMP error message-Destination Unreachable.

French Abstract
L'invention concerne un procede et un appareil destines a des tests de recevabilite et a des tests d'accessibilite de paquets multidestination explicite. Le test de recevabilite multidestination selon l'invention comprend les etapes suivantes : a un terminal emetteur, envoi d'un paquet test de recevabilite a un terminal recepteur ; au terminal recepteur, reception du paquet test de recevabilite ; generer un message d'erreur ICMP destination inaccessible ; emission du message d'erreur ICPM destination inaccessible au terminal emetteur ; au terminal emetteur, reception dudit message d'erreur ; et analyse du message d'erreur ICPM destination inaccessible.

Legal Status (Type, Date, Text)
Publication 20040205 A1 With international search report.

Fulltext Availability:
Detailed Description
Claims

Detailed Description
... address, which is specially assigned for xcast, as a
7
destination address. Also, because TFL(**Time** -to- **Live**) value in the **tunnel** IP header of the reachability probe packet P 500 is set in proportion to the number of generation of probe packet, the validity of **TTL** value is checked every time the probe packetpasses through each router, transit node.

FIGA shows...

Claim
... is not capable of I 0 the explicit multicasting from the n routers by analyzing **TTL** value.

12 The method as stated in claim 9, wherein the reachability probe packet comprises a **tunnel** IP header, a **tunnel** explicit multicast header and a receivability probe packet.

13 The method as stated in claim...
?t9/5,k/8-17,19-23

9/5,K/8 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01086242 **Image available**
REAL-TIME PACKET TRACEBACK AND ASSOCIATED PACKET MARKING STRATEGIES
TRACAGE EN TEMPS REEL DE PAQUETS ET STRATEGIES DE MARQUAGE DE PAQUETS ASSOCIEES

Patent Applicant/Assignee:
THE PENN STATE RESEARCH FOUNDATION, 304 Old Main, University Park, PA 16802-7000, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
HAMADEH Ihab, 711 University Drive, Apt # S209, State College, PA 16801, US, US (Residence), LB (Nationality), (Designated only for: US)
KESIDIS George, 692 Tanager Drive, State College, PA 16803, US, US (Residence), CA (Nationality), (Designated only for: US)
Legal Representative:
GEORGE Keith E (et al) (agent), McDermott, Will & Emery, 600 13th Street, N.W., Washington, DC 20005-3096, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200408700 A2 20040122 (WO 0408700)
Application: WO 2003US21845 20030711 (PCT/WO US03021845)
Priority Application: US 2002395838 20020712; US 2003470337 20030514
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/56
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 21592

English Abstract
To facilitate effective and efficient tracing of packet flows back to a trusted point as near as possible to the source of the flow in question, devices on the border of the trusted region are configured to mark packets with partial address information. Typically, the markings comprise fragments of IP addresses of the border devices in combination with fragment identifiers. By combining a small number of marked packets, victims or other interested parties are able to reconstruct the IP address of each border device that forwarded a particular packet flow into the trusted region, and thereby approximately locate the source(s) of traffic without requiring the assistance of outside network operators. Moreover, traceback can be done in real-time, e.g. while a DDoS attack is on-going, so that the attack can be stopped before the victim suffers serious damage.

French Abstract
L'invention concerne des dispositifs situes sur la limite de la region fiable qui sont configures pour marquer des paquets au moyen d'informations partielles d'adresse, de maniere a faciliter et tracer de maniere efficace des flux de paquets retournant a un point fiable aussi pres que possible de la source du flux en question. Generalement, les marquages comprennent des fragments d'adresses IP des dispositifs de la limite, conjointement avec des identificateurs de fragments. La combinaison d'un petit nombre de paquets marques, de victimes ou de

parties interessees permet de reconstruire l'adresse IP de chaque dispositif de la limite ayant transmis un flux de paquets specifique dans la region fiable et localisant ainsi de maniere approximativement la ou les sources de trafic, sans necessiter l'aide d'operateurs de reseau externes. De plus, le tracage peut etre effectue en temps reel, par exemple, pendant une attaque DDoS, de maniere que l'attaque puisse etre arretee avant que la victime ne presente des dommages importants.

Legal Status (Type, Date, Text)
Publication 20040122 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Detailed Description

Detailed Description

9/5,K/9 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01077196 **Image available**
METHOD AND APPARATUS FOR ENHANCED SECURITY FOR COMMUNICATION OVER A NETWORK
PROCEDE ET APPAREIL PERMETTANT D'OBTENIR UNE PLUS GRANDE SECURITE DE COMMUNICATION SUR UN RESEAU
Patent Applicant/Assignee:
NVIDIA CORPORATION, 2701 San Tomas Expressway, Santa Clara, CA 95050, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
MAUFER Thomas Albert, 20050 Rodrigues Ave., "B", Cupertino, CA 95014, US, US (Residence), US (Nationality), (Designated only for: US)
NANDA Sameer, 377 Kincora Court, San Jose, CA 95136, US, US (Residence), IN (Nationality), (Designated only for: US)
SIDENBLAD Paul J, 10190 Stonydale Drive, Cupertino, CA 95014, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
PATTERSON Todd B (agent), Moser, Patterson & Sheridan LLP, 3040 Post Oak Boulevard, Suite 1500, Houston, TX 77056, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 2003107624 A1 20031224 (WO 03107624)
Application: WO 2003US17502 20030603 (PCT/WO US0317502)
Priority Application: US 2002172352 20020613; US 2002172683 20020613; US 2002172046 20020613; US 2002172345 20020613
Parent Application/Grant:
Related by Continuation to: US 2002172352 20020613 (CIP)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
International Patent Class: H04L-029/12
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 15370
English Abstract
Method and apparatus for Internet Protocol Security (IPSec) and Network Address Translation (NAT) integration is described. Additionally, method and apparatus for enhanced security for communication over a network, and

more particularly to control of security protocol negotiation to enable multiple clients to establish a virtual private network connection with a same remote address, is described. Furthermore, method and apparatus for enhanced security for communication over a network, and more particularly to NAT integration IPSec, is described. Moreover, method and apparatus for integration of NAT and source address security, including, but not limited to, determining whether a gateway computer is integrated for NAT and source address security, is described.

French Abstract
L'invention concerne un procede et un appareil d'integration de la securite du protocole internet (IPSec) et de la traduction d'adresse de reseau (NAT). L'invention concerne egalement un procede et un appareil assurant une plus grande securite de communication sur un reseau, et plus particulierement le controle de la negociation du protocole de securite pour permettre a de multiples clients d'etablir une connexion de reseau privee virtuelle avec une meme adresse eloignee. L'invention concerne, de plus, un procede et un appareil permettant d'obtenir une plus grande securite de communication sur un reseau, et plus particulierement l'integration d'IPSec a NAT. L'invention concerne en outre un procede et un appareil d'integration de NAT et de la securite d'adresse source, consistant, entre autres, a determiner si un ordinateur a passerelle est integre pour NAT et la securite d'adresse source.

Legal Status (Type, Date, Text)
Publication 20031224 A1 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... MAC address as the MAC address in the packet's MAC Source Address field, then **IPSec** packet is transmitted unchanged by the NAT gateway computer (except for decrementing the **TTL** and updating the IP checksum in the case of IPv4 packets; IPv6 packets are plentiful...

9/5,K/10 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01075944
GIGABIT ETHERNET ADAPTER SUPPORTING THE ISCSI AND IPSEC PROTOCOLS
ADAPTATEUR ETHERNET GIGABIT SUPPORTANT LES PROTOCOLES ISCSI ET IPSEC
Patent Applicant/Assignee:
IREADY CORPORATION, 2903 Bunker Hill Lane, Suite 202, Santa Clara, CA 95054, US, US (Residence), US (Nationality)
Inventor(s):
MINAMI John Shigeto, 66 Queen Street #2602, Honolulu, HI 96813, US,
UYESHIRO Robin Yasu, 1234 Kelewina St., Kailua, HI 96734, US,
JOHNSON Michael Ward, 482 Knottingham Circle, Livermore, CA 94550, US,
SU Steve, 3420 Oahu Avenue, Honolulu, HI 96822, US,
SMITH Michael John Sebastian, 825 Lima Court, Palo Alto, CA 94306, US,
CHEN Addison Kwuanming, 2121 Algaroba St. Apt. 905, Honolulu, HI 96826, US,
DOCTOR Mihir Shaileshbhai, 2231 Ala Wai Blvd. #202, Honolulu, HI 96815, US,
GREENFIELD Daniel Leo, 2115 Ala Wai Blvd., Apt. 1001, Honolulu, HI 96815, US,
Legal Representative:
GLENN Michael (et al) (agent), Glenn Patent Group, 3475 Edison Way, Ste. L., Menlo Park, CA 94025, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 2003105011 A1 20031218 (WO 03105011)
Application: WO 2003US18049 20030606 (PCT/WO US0318049)
Priority Application: US 2002386924 20020606; US 2003456871 20030605
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT
RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE
SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-015/16
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 56137

English Abstract
The invention is embodied in a gigabit Ethernet adapter. A system according to the invention provides a compact hardware solution to handling high network communication speeds. In addition, the invention adapts to multiple communication protocols via a modular construction and design.

French Abstract
L'invention porte sur un adaptateur Ethernet gigabit. Un systeme de cette invention donne une solution materielle compacte au traitement a hautes vitesses de la communication sur reseau. De plus, l'invention s'adapte a de multiples protocoles de communication via une construction et une conception modulaires.

Legal Status (Type, Date, Text)
Publication 20031218 A1 With international search report.
Publication 20031218 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

Fulltext Availability:
Detailed Description
Detailed Description

9/5,K/11 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01073269 **Image available**
SERVICE PROCESSING SWITCH AND CORRESPONDING METHOD
COMMUTATEUR DE TRAITEMENT DE SERVICES ET PROCEDE CORRESPONDANT
Patent Applicant/Assignee:
COSINE COMMUNICATIONS INC, 1200 Bridge Parkway, Redwood City, CA 94065, US, US (Residence), US (Nationality)
Patent Applicant/Inventor:
HUSSAIN Zahid, 5358 Laurel Canyon Drive, San Jose, CA 95138, US, US (Residence), US (Nationality), (Designated only for: US)
MILLET Tim, 621 Lola Lane, Mountain View, CA 94040, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
STEFFEY Charles E (et al) (agent), Schwegman, Lundberg, Woessner & Kluth, P.O. Box 2938, Minneapolis, MN 55402, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 2003103238 A1 20031211 (WO 03103238)
Application: WO 2003US17675 20030604 (PCT/WO US0317675)
Priority Application: US 2002163260 20020604
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW (EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/56
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 8646

English Abstract
A system and method for providing IP services. A packet is received at a line interface/network module and forwarded to a virtual routing engine. The virtual routing engine determines if the packet requires processing by a virtual service engine. If the packet requires processing by the virtual services engine, the packet is routed to the virtual services engine for processing.
French Abstract
L'invention concerne un systeme et un procede permettant de fournir des services IP. Un module interface de ligne/reseau recoit un paquet qui est transmis a un moteur d'acheminement virtuel. Ce dernier determine si le paquet necessite un traitement par un moteur de service virtuel. Si tel est le cas, ledit paquet est achemine vers le moteur de service virtuel pour traitement.

Legal Status (Type, Date, Text)
Publication 20031211 A1 With international search report.
Publication 20031211 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

Fulltext Availability:
Detailed Description

Detailed Description

9/5,K/12 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01061259 **Image available**
A METHOD AND SYSTEM FOR FORWARDING DATA UNITS
PROCEDE ET SYSTEME DE RETRANSMISSION D'UNITES DE DONNEES
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
KOKKONEN Jani, Ruorikuja 2 D 43, FIN-02320 Espoo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
VESTERINEN Seppo, Lillukkakuja 8, FIN-90460 Oulunsalo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
PAPULA OY (agent), P.O. Box 981, FIN-00101 Helsinki, FI,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200392226 A1 20031106 (WO 0392226)
Application: WO 2003FI204 20030318 (PCT/WO FI0300204)
Priority Application: FI 2002791 20020424
Designated States: AE AG AL AM AT (utility model) AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ (utility model) CZ DE (utility model) DE DK (utility model) DK DM DZ EC EE (utility model) EE ES FI (utility model) FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK (utility model) SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/56
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 7719

English Abstract
A method and system for forwarding data units in a communications system, that comprises: ingress routers (901) capable of forwarding data units and containing a Forwarding Equivalence Class table (911) that contains mapping information, intermediate routers (905, 907, 909) capable of forwarding data units, egress routers (903) capable of forwarding data and containing a Forwarding Equivalence Class table (919) that contains mapping information. The method comprising the steps of: assigning a first label on data unit and a second label on data unit based on mapping information, sending data unit in to egress router via one or more intermediate router (905, 907, 909), receiving (903) data unit, identifying data unit based on mapping information on Forwarding Equivalence Class table (919) and based on second label. The method further comprises the steps of: creating a Forwarding Equivalence Class for radio access network specific data units; and storing information about Forwarding Equivalence Class in Forwarding Equivalence class table (FEC).

French Abstract
La presente invention a trait a un procede et un systeme de retransmission d'unites de donnees dans un systeme de communications, comportant : des routeurs d'entree (901) aptes a la retransmission d'unites de donnees et contenant une table de classe d'equivalence de retransmission (911) qui contient une information de correspondance geographique, des routeurs intermediaires (905, 907, 909) aptes a la retransmission d'unites de donnees, des routeurs de sortie (903) aptes a la retransmission de donnees et contenant une table de classe d'equivalence de retransmission (919) qui contient une information de correspondance geographique. Le procede comprend les etapes suivantes : l'attribution d'une premiere etiquette a une unite de donnees et d'une deuxieme etiquette a l'unite de donnees en fonction de l'information de correspondance geographique, l'envoi de l'unite de donnees a un routeur de sortie via un ou des routeurs intermediaires (905, 907, 909), la reception (903) de l'unite de donnees, l'identification de l'unite de donnees en fonction de l'information de correspondance geographique sur la table de classe d'equivalence de retransmission et en fonction de la deuxieme etiquette. Le procede comprend en outre les etapes suivantes : la creation d'une classe d'equivalence de retransmission pour des unites de donnees specifiques de reseau d'acces radio ; et le stockage de donnees concernant la classe d'equivalence de retransmission dans la table de classe d'equivalence de retransmission.

Legal Status (Type, Date, Text)
Publication 20031106 A1 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description

9/5,K/13 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01057878 **Image available**
PROCESSING A PACKET USING MULTIPLE PIPELINED PROCESSING MODULES
TRAITEMENT DE PAQUET AU MOYEN DE MODULES DE TRAITEMENT PIPELINES MULTIPLES

Patent Applicant/Assignee:
HI FN INC, 750 University Avenue, Los Gatos, CA 95032-7695, US, US (Residence), US (Nationality)
Inventor(s):
SAVARDA Raymond, 4224 Sancroft Drive, Apex, NC 27502, US,
BLAKER David, 109 Hogan Glen Court, Chapel Hill, NC 27516, US,
WINKELSTEIN Dan, 2308 Lawrence Drive, Raleigh, NC 27603, US,
Legal Representative:
MYERS BIGEL SIBLEY & SAJOVEC P A (agent), P.O. Box 37428, Raleigh, NC 27627, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200388072 A1 20031023 (WO 0388072)
Application: WO 2003US10545 20030408 (PCT/WO US0310545)
Priority Application: US 2002120577 20020411
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-015/80
International Patent Class: H04L-012/56; H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 11500

English Abstract
A packet is processed by encapsulating the packet with a packet-object header if the packet does not have a packet-object header. The encapsulated packet is processed based on information contained in the packet-object header using a plurality of transform modules that are coupled to each other in a series or pipeline configuration. The plurality of transform modules process the encapsulated packet independent of each other.

French Abstract
Selon l'invention, un paquet est traite par encapsulation avec un en-tete d'objets de paquet si ledit paquet ne comporte pas d'en-tete d'objets de paquet. Le paquet encapsule est traite en fonction d'informations contenues dans ledit en-tete d'objets de paquet, au moyen d'une pluralite de modules de transformation couples les uns aux autres en serie ou selon une configuration pipeline. La pluralite de modules de transformation traite les paquets encapsules, independamment les uns des autres.

Legal Status (Type, Date, Text)
Publication 20031023 A1 With international search report.
Publication 20031023 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20031224 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... SAD lookup module 118.

The outbound pre-crypto module 122 may be configured to handle **time** -to-**live** (**TTL**) decrement operations, pre-cryptographic fragmentation, and insertion of **IPSec** information into the crypto header 215. In more detail, the outbound pre-crypto module 122...

9/5,K/14 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01033401 **Image available**
METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
PROCEDE ET SYSTEME D'ENVOI D'UN MESSAGE PAR UNE CONNEXION SECURISEE
Patent Applicant/Assignee:
INTRASECURE NETWORKS OY, PL 38, FIN-02201 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
VAARALA Sami, Neljas Linja 22 A, FIN-00530 Helsinki, FI, FI (Residence), FI (Nationality), (Designated only for: US)
NUOPPONEN Antti, Kaksoiskiventie 7-9 A 1, FIN-02760 Espoo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
INNOPAT LTD (agent), P.O. Box 556, FIN-02151 Espoo, FI,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200363443 A1 20030731 (WO 0363443)
Application: WO 2003FI45 20030121 (PCT/WO FI0300045)
Priority Application: FI 2002112 20020122
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
International Patent Class: H04Q-007/38
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 13623

English Abstract
The method and system of the invention enable secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. It is mainly characterized in that a message is formed in the first computer or in a computer that is served by the first computer, and in the latter case, sending the message to the first computer. In the first computer, a secure message is then formed by giving the message a unique identity and a destination address. The message is sent from the first computer to the intermediate computer, whereafter said destination address and the unique identity are used to find an address to the second computer. The current destination address is substituted with the found address to the second computer, and the unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

French Abstract
L'invention concerne un procede et un systeme qui permettent d'envoyer de maniere securisee un message a partir d'un premier ordinateur vers un second ordinateur par le biais d'un ordinateur intermediaire sur un reseau de telecommunications. Lesdits procede et systeme se caracterisent principalement en ce qu'un message est forme dans le premier ordinateur ou dans un ordinateur servi par le premier ordinateur et, en l'occurrence, ledit ordinateur envoie le message au premier ordinateur. Dans le premier ordinateur, on forme un message securise en lui donnant une identite unique et une adresse de destination. Le message est envoye du premier ordinateur vers l'ordinateur intermediaire; lesdites adresse de destination et identite unique sont ensuite utilisees pour trouver une

adresse au second ordinateur. L'adresse de destination en cours est remplacee par l'adresse trouvee pour le second ordinateur, et l'identite unique par une autre identite unique. Le message est alors envoye au second ordinateur.

Legal Status (Type, Date, Text)
Publication 20030731 A1 With international search report.
Publication 20030731 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20031016 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... integrity check value calculation, except possibly for fields not covered by. AH (such as.- the- **Time** -Tom- **Live** field, the- header. checksurrL etc). Thus, the AH integrity check value is now correct.

In step 3, the second computer performs standard **IPSec** processing of AH. The packet, which now is uncovered from the tunnel is sent to...

9/5,K/15 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01015049 **Image available**
OPTICALLY BOOSTED ROUTER
ROUTEUR A RENFORCEMENT OPTIQUE
Patent Applicant/Assignee:
UNIVERSITY OF SOUTHERN CALIFORNIA, 3716 S. Hope Street, #313, Los Angeles, CA 90007-4344, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
BANNISTER Joseph, 4224 Via Pinzon, Palos Verdes Estates, CA 90274, US, US (Residence), US (Nationality), (Designated only for: US)
TOUCH Joseph D, 1101 John Street, Manhattan Beach, CA 90266, US, US (Residence), US (Nationality), (Designated only for: US)
KAMATH Purushotam, 947 West 30th Street, Apt. 22, Los Angeles, CA 90007, US, US (Residence), IN (Nationality), (Designated only for: US)
PATEL Aatash, **, **, -- (Residence), -- (Nationality), (Designated only for: US)
Legal Representative:
HARRIS Scott C (et al) (agent), Fish & Richardson P.C., Suite 500, 4350 La Jolla Village Drive, San Diego, CA 92122, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200344998 A2-A3 20030530 (WO 0344998)
Application: WO 2002US36783 20021115 (PCT/WO US02036783)
Priority Application: US 2001334673 20011115
Parent Application/Grant:
Related by Continuation to: US 2001334673 20011115 (CON)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04Q-011/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims

Fulltext Word Count: 7358

English Abstract
Systems and techniques to optically boost a router. In general, in one implementation, the technique includes: receiving an optical signal defining a packet of data, initiating electronic routing of the optical packet, and initiating optical routing of the optical packet. The optical routing involves determining forwarding information based on a routing field in the optical packet, and if optical forwarding is available, terminating the electronic routing of the packet before completion of the electronic routing and forwarding the optical signal, which defines the packet, based on the determined forwarding information.

French Abstract
Cette invention concerne des systemes et des techniques permettant de renforcer optiquement un routeur. De facon generale, et dans un mode de realisation, la technique consiste a : recevoir un signal optique definissant un paquet de donnees, lancer le routage electronique du paquet optique et lancer le routage optique du paquet optique. Le routage optique passe par les operations suivantes : determination de l'information d'acheminement a partir d'un champ d'acheminement dans le paquet optique ; et, si l'acheminement optique est possibles, terminer le routage electronique du paquet avant achevement du routage electronique et transmission du signal optique, lequel definit le paquet, en fonction de l'information d'acheminement determinee.

Legal Status (Type, Date, Text)
Publication 20030530 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20040219 Late publication of international search report
Republication 20040219 A3 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... and addresses that correspond to the router itself, such as an endpoint of an IP **tunnel** , can be ignored.

[00631 FIG. 8 shows a conceptual diagram of an optical **TTL** decrement module 520. Packets with **TTL** fields within the header (not necessarily at the start of the header, but contained within...

9/5,K/16 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01013272 **Image available**
PHYSICALLY SCOPED MULTICAST IN MULTI-ACCESS NETWORKS
MULTI-DIFFUSION A LIMITATION DE PORTEE PHYSIQUE DANS UN RESEAU MULTI-ACCES
Patent Applicant/Assignee:
NOKIA INC, 6000 Connection Drive, Irving, TX 75039, US, US (Residence), US (Nationality)
Inventor(s):
TROSSEN Dirk, 300 Mystic Valley Parkway, Arlington, MA 02474, US,
KRISHNAMURTHI Govind, 276 Massachusetts Avenue, #105, Arlington, MA 02474, US,
CHASKAR Hemant, 111 Locust Street, Apartment 40-C-1, Woburn, MA 01801, US,
Legal Representative:
WRIGHT Bradley C (agent), Banner & Witcoff, Ltd., 1001 G Street, N.W., Eleventh Floor, Washington, DC 20001-4597, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200343241 A1 20030522 (WO 0343241)
Application: WO 2002IB4695 20021108 (PCT/WO IB0204695)
Priority Application: US 2001987198 20011113

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU
CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04J-003/24
International Patent Class: H04J-003/26; H04L-012/56
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6916

English Abstract
An apparatus and method is provided for forwarding multicast packets (Fig. 2A) in a communication network using a physically scoped routing protocol. Each of a plurality of access routers maintains information concerning the addresses of physically neighboring access routers. Multicast packets received by each access router are evaluated to determine whether they should be routed using a conventional administratively scoped routing rule or using a physically scoped routing rule. Administratively scoped packets are routed to the multicast address using conventional administrative scoping rules. Physically scoped packets are " **tunneled** " by encapsulating them in a unicast packet, which is then transmitted to one or more physically neighboring access routers. An optional **time** -to- **live** parameter allows multiple levels of neighboring proximity to be specified.

French Abstract
Cette invention concerne un dispositif et un procede permettant d'acheminer des paquets multi-diffusion (fig. 2A) dans un reseau de communication au moyen d'un protocole de routage a limitation de portee physique. Chacun de la pluralite des routeurs de bordure renferme des informations sur les adresses de routeurs de bordure accessibles physiquement. Les paquets multi-diffusion recus par chaque routeur de bordure font l'objet d'une evaluation visant a determiner s'ils doivent etre achemines selon une regle de limitation de portee administrative classique ou d'une regle de routage a limitation de portee physique. Les paquets a limitation de portee administrative sont achemines vers le reseau mutli-acces conformement a des regles de limitation de portee administrative classiques. Les paquets a limitation de portee physique sont canalises sous forme d'un paquet uni-diffusion encapsule qui est ensuite transmis a un ou a plusieurs routeurs d'acces avoisinants. On peut eventuellement utiliser un parametre de temps de vie pour specifier des niveaux multiples de proximite de voisinage.

Legal Status (Type, Date, Text)
Publication 20030522 A1 With international search report.
Publication 20030522 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20030814 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description
Claims

English Abstract
...are routed to the multicast address using conventional administrative scoping rules. Physically scoped packets are " **tunneled** " by encapsulating them in a unicast packet, which is then transmitted to one or more physically neighboring access routers. An optional **time** -to- **live** parameter allows multiple levels of neighboring proximity to be

specified.

Detailed Description
... router includes both a packet forwarding function 201 as shown in FIG. 2A and a **tunneled** packet handling function 212 as shown in FIG. 2B.

1311 Incoming **tunneled** multicast packets 218, 219, 220 are received at a **time** -to- **live** handier function 214, which extracts and decrements the **TTL** parameter in each packet. It is assumed that each **tunneled** packet comprises a normal unicast header and the original multicast packet. (Although not explicitly shown...from the originating sender. This process is repeated at each receiving access router until the **TTL** field is zero.

134] FIG. 3B ...carrying out steps corresponding to the structure shown in FIG. 2B. In step 307, the **tunneled** multicast packet is received in the access router.

ID step 308, the **TTL** parameter is extracted from die packet and decremented. In step 309, the original multicast packet...
...the access router (e.g., printer servers or other devices). If in step 311 the **TTL** parameter is not greater than zero, then processing is completed per step 312.

Otherwise, in step 313, the **tunneled** multicast packet is replicated and forwarded to all physical neighbors within the physical neighborhood scope...

Claim
... multicast data packet, de-encapsulating the tunneled multicast data packet and forwardmig the de-encapsulated **tunneled** multicast data packet to devices locally connected to the network
access device; and
(4) in response to determining that a **time** -to- **live** parameter in the unicast data packet is greater than a predetermined value, replicating the unicast...

9/5,K/17 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00967926 **Image available**
SYSTEM AND METHOD FOR MANAGING SECURITY PACKET PROCESSING
SYSTEME ET PROCEDE POUR LA GESTION DU TRAITEMENT DES PAQUETS DE SECURITE IPSEC
Patent Applicant/Assignee:
CORRENT CORPORATION, 1711 West Greentree Drive, Suite 201, Tempe, AZ 85283, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
NOEHRING Lee P, 22415 North 67th Drive, Glendale, AZ 85310, US, US (Residence), US (Nationality), (Designated only for: US)
MERCER Chad W, 287 East Hampton Lane, Gilbert, AZ 85296, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
STEFFEY Charles E (et al) (agent), Schwegman, Lundberg, Woessner & Kluth, P.O. Box 2938, Minneapolis, MN 55402, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 2002102027 A1 20021219 (WO 02102027)
Application: WO 2002US19081 20020612 (PCT/WO US0219081)
Priority Application: US 2001297646 20010612; US 2002160330 20020530
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
International Patent Class: H04L-012/28
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 17673

English Abstract
An IPSec packet processing system includes an IPSec manager to interface with an IPSec engine, to manage memory and to handle exceptions associated with IPSec packet processing. The IPSec managermay be a software module operating as part of a software stack on a host processor while the IPSec engine may perform IPSec packet processing. The IPSec manager may also initiate the negotiation of new keys, send ICMP messages for PMTU violations and log entries for exceptions.

French Abstract
L'invention concerne un systeme de traitement de paquets IPSec, qui comprend un gestionnaire IPSec assurant l'interface avec un moteur IPSec, la gestion de memoire, et la prise en charge des exceptions associees au traitement des paquets IPSec. Le gestionnaire IPSec peut etre un module logiciel mis en oeuvre dans le cadre d'une pile logicielle sur un processeur hote, et le moteur IPSec peut accomplir le traitement des paquets IPSec. En outre, le gestionnaire IPSec peut engager la negociation relative a l'utilisation de nouvelles cles, transmettre des messages de protocole ICMP correspondant aux violations d'unite de transmission maximum en paquet (PMTU) et enregistrer les entrees correspondant aux exceptions.

Legal Status (Type, Date, Text)
Publication 20021219 A1 With international search report.
Publication 20021219 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Fulltext Availability:
Detailed Description

Detailed Description
... Outbound SAD table entry 600 (FIG. 6) may also include hard byte lifetime field 616, **TTL** /hop field 618, SPI number field 620, **tunnel** source address field 624, **tunnel** destination address field 626 and reserved fields 628.

Finnware of lPSec engine 104 may

9/5,K/19 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00907427 **Image available**
A COMMUNICATIONS SYSTEM
SYSTEME DE COMMUNICATIONS
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02510 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
KOKKONEN Jani, Meiramikuja 3C10, FIN-02940 Espoo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
SLINGSBY Philip Roy (agent), Page White & Farrer, 54 Doughty Street, London WC1N 1LS (et al), GB,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200241589 A1 20020523 (WO 0241589)
Application: WO 2001EP12774 20011105 (PCT/WO EP0112774)
Priority Application: GB 200027985 20001116
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/56
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 5455

English Abstract
A communication system for transferring data packets between a network device located within a first network and a network device located within a second network. The data packets having a header allowing each packet to be routed independently through each node of the second network using routing information to process the header of each incoming data packet and forward the data packet to the next node. The headers of each of said data packets entering said first network at an ingress node are encapsulated by assigning at least one label to each data packet so that the data packets can be forwarded by each of the intermediate nodes based on said label without having to process the header information.

French Abstract
La presente invention concerne un systeme de communications qui permet de transferer des paquets de donnees entre un dispositif de reseau situe a l'interieur d'un premier reseau et un dispositif de reseau situe a l'interieur d'un second reseau. Les paquets de donnees comprennent un en-tete qui permet d'acheminer chaque paquet independamment a travers chaque noeud du second reseau a l'aide d'informations d'acheminement qui permettent de traiter l'en-tete de chaque paquet de donnees en entree et de retransmettre le paquet de donnees au noeud suivant. Les en-tetes de chacun des paquets de donnees precites arrivant au premier reseau par un noeud d'entree sont encapsules, chacun d'eux recevant au moins une etiquette de facon que les paquets de donnees peuvent etre retransmis par chacun des noeuds intermediaires sur la base de l'etiquette sans qu'il soit necessaire de traiter les informations contenues dans l'en-tete.

Legal Status (Type, Date, Text)
Publication 20020523 A1 With international search report.
Publication 20020523 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20021114 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... is assigned to the user packet to identify the MS inside the top level LSP- **tunnel** . In this case, the **TTL** field of the label is not used as a normal hop counter, but rather as...Sub-Network Dependent Convergence Protocol
TCP - Transmission Control Protocol
TDMA- Time Division Multiple Access
TEI - **Tunnel** Endpoint Identifier
TTL - **Time** To **Live**
UDP - User Datagram Protocol
UIM - User Identity Module (UMTS)

UMTS - Universal Mobile Telecommunications System
UTRAN...

9/5,K/20 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00905545 **Image available**
SWITCH-BASED NETWORK PROCESSOR
PROCESSEUR DE RESEAU A BASE D'UN COMMUTATEUR
Patent Applicant/Assignee:
FAST-CHIP INC, 950 Kifer Road, Sunnyvale, CA 94086-05206, US, US (Residence), US (Nationality)
Inventor(s):
HENDERSON Alex E, 40 Denise Drive, Hillsborough, CA 94010, US,
CROFT Walter E, 2311 Ticonderoga Drive, San Mateo, CA 94402, US,
Legal Representative:
SMITH Jeff (et al) (agent), Fenwick & West LLP, Two Palo Alto Square, Palo Alto, CA 94306, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200239667 A2-A3 20020516 (WO 0239667)
Application: WO 2001US46297 20011107 (PCT/WO US0146297)
Priority Application: US 2000246790 20001107
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/56
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6094

English Abstract
A switch-based network processor is disclosed. The switch-based network processor includes a packet parser, search and modification scheduler that parses a data packet, develops a search for a processing rule associated with the packet, and schedules a modification to be performed on the packet based on the rule. The processor also includes several search resources that each can search simultaneously for a processing rule. Multiple packet modifiers are included to modify several packets simultaneously. a core switch is also provided to switch search requests from the parser to the search resources, to switch search responses from the search resources to the parser, and to switch modification requests and responses between the parser and packet modifiers. The switch-based processor also includes a session state storage device that can be used to allow the processor to be aware of a session.

French Abstract
L'invention porte sur un commutateur de reseau a base d'un commutateur qui comprend un analyseur de paquets, un programmateur de recherche et de modification qui analyse un paquet de donnees, developpe une recherche pour une regle de traitement associee au paquet, et programme une modification a effectuer sur le paquet sur la base de la regle. Le processeur comprend egalement plusieurs ressources de recherche qui peuvent rechercher chacune simultanement une regle de traitement. Plusieurs modificateurs de paquets permettent de modifier simultanement plusieurs paquets. Un commutateur central permet de commuter des demandes de recherche de l'analyseur aux ressources de recherche, de commuter des reponses des ressources de recherche a l'analyseur et de commuter des demandes de modification et des reponses entre l'analyseur et les

modificateurs de paquets. Le processeur a base de commutateur comprend egalement une memoire d'etat de session qui peut etre utilisee pour que le processeur puisse reconnaitre une session.

Legal Status (Type, Date, Text)
Publication 20020516 A2 Without international search report and to be republished upon receipt of that report.
Examination 20021017 Request for preliminary examination prior to end of 19th month from priority date
Correction 20030417 Corrected version of Pamphlet: pages 1/6-6/6, drawings, replaced by new pages 1/6-6/6; due to late transmittal by the receiving Office
Republication 20030417 A2 Without international search report and to be republished upon receipt of that report.
Correction 20030417 Corrected version of Pamphlet:
Search Rpt 20030821 Late publication of international search report
Republication 20030821 A3 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... using the switch-based processor. For example, multi-protocol label switching (MTLS), push, pop, merge, **time** to **live** (**TTL**) decrement, and Internet protocol (IP) checksum recalculate modifications may be executed. Also, encryption extensions that use modification for **IPSEC** (**IP security**) "mutable" fields, support for source routing, and IP checksum recalculation, may be performed by the...

9/5,K/21 (Item 15 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00857661 **Image available**
METHOD AND SYSTEM FOR STOPPING HACKER ATTACKS
PROCEDE ET SYSTEME PERMETTANT LA MISE EN OEUVRE DE FONCTIONS DE PROTECTION CONTRE LES ATTAQUES ENTRAINANT UN REFUS DE PRESTATION DE SERVICES ET L'ANALYSE DU TRAFIC DANS LE CADRE DES RESEAUX PRIVES VIRTUELS BASES IP ET DISTRIBUTION DE DONNEES VIA L'UTILISATION D'UNE TECHNIQUE DE SAUT D'ADRESSES MULTICAST IP
Patent Applicant/Assignee:
LADR IT CORPORATION, 6 Sawgrass Circle, Ashton, Ontario K0A 1B0, CA, CA (Residence), CA (Nationality)
Inventor(s):
SHAWCROSS Charles Byron Alexander, 6 Sawgrass Circle, Ashton, Ontario K0A 1B0, CA,
Legal Representative:
CASSAN Lynn S (et al) (agent), Cassan MacLean, 401 - 80 Aberdeen Street, Ottawa, Ontario K1S 5R5, CA,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200191397 A2-A3 20011129 (WO 0191397)
Application: WO 2001CA727 20010522 (PCT/WO CA0100727)
Priority Application: US 2000575544 20000522
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/18
International Patent Class: H04L-012/46
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description

Claims
Fulltext Word Count: 12268

English Abstract
A method and system for Internet Protocol network communications and uses thereof for protecting Internet sites against denial of service and traffic analysis attacks on insecure public networks such as the Internet are provided. The method provides for communicating multicast packets between end stations, in a multicast IP network, on a chosen multicast IP address from a plurality of multicast IP addresses for multicast communication using a multicast address hopping technique. The technique selectively varies the chosen multicast IP address from the plurality of multicast IP addresses according to a predetermined scheme known to the end stations but not to unauthorized endstations. The packets are then communicated on the chosen multicast IP address. Indicia normally capable of identifying the source of the packets may be selectively varied to conceal the source of the packets. Further, use of the invention for Virtual Private Networks is also provided.

French Abstract
L'invention concerne un procede et un systeme ayant trait aux communications par reseau Internet et leur utilisation pour la protection des sites Internet contre les attaques entrainant un refus de prestation de services et l'analyse du trafic sur les reseaux publics non securises, notamment l'Internet. Ledit procede consiste, dans le cadre d'un reseau IP multicast, a communiquer des paquets multipoint entre stations terminales, sur une adresse multicast IP choisie parmi une pluralite d'adresses, aux fins d'une communication multipoint par une technique de saut d'adresses multicast. Cette technique modifie selectivement l'adresse multicast IP choisie parmi la pluralite d'adresses precitee selon une logique predeterminee connue des stations terminales mais non connue des stations terminales non autorisees. Les paquets sont ensuite communiques sur l'adresse multicast IP choisie. Les indices permettant normalement d'identifier la source des paquets peuvent etre modifies selectivement, de maniere a masquer la source desdits paquets. En outre, les paquets peuvent etre communiques a une station terminale ayant souscrit a un ensemble d'adresses multicast IP comprenant non seulement au moins une adresse multicast IP appartenant a la pluralite d'adresses IP precitee aux fins d'une communication multipoint, mais aussi l'adresse multicast IP choisie pour la transmission des paquets. Cet ensemble d'adresses multicast IP peut egalement etre selectivement modifie selon une logique predeterminee secrete connue des stations terminales, notamment par son adjonction et sa suppression aleatoire a/de l'ensemble des adresses IP multipoint. Plusieurs ensembles de groupes de communication, utilisant tous le meme espace d'adressage, peuvent ainsi coexister, de sorte que leur trafic respectif soit enchevetre dans les diverses adresses, ce qui rend l'analyse du trafic particulierement difficile. Dans un autre mode de realisation, une logique de codage de donnees, tel que le multiplexage par repartition de code, peut etre utilisee pour chaque champ de donnees des paquets multicast de maniere a permettre aux donnees destinees a des destinations differentes d'etre melangees en un seul paquet, qui sera diffuse a une pluralite de recepteurs. Chaque recepteur decode alors les donnees qui le concernent par l'application de la logique de decodage appropriee, notamment un demultiplexage par division de code, au champ de donnees multicast. D'autres aspects de l'invention concernent les reseaux prives virtuels et autres systemes de communication securises.

Legal Status (Type, Date, Text)
Publication 20011129 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20020808 Late publication of international search report
Republication 20020808 A3 With international search report.

Fulltext Availability:
Claims

Claim

... claim 1 wherein the indicia are chosen from the group comprising a Time To Life (**TTL**) field and a IP Source Address field of the multicast packets.

4 The method of claim 1 further inciuding the step of **tunneling** the multicast packets according to a network protocol to one or more tunnel exii hosts...claim 16 wherein the indicia are chosen from the group comprising a Time To Life (**TTL**) field and a IP Source Address field of the multicast packets.

19 The system of claim 16 further including means for **tunneling** the multicast packets according to a network protocol to one or more tunnel exit hosts...

9/5,K/22 (Item 16 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00789121 **Image available**
PACKET NETWORK INTERFACING
INTERFACAGE DE RESEAU DE PAQUETS
Patent Applicant/Assignee:
BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY, 81 Newgate Street, London EC1A 7AJ, GB, GB (Residence), GB (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
HOVELL Peter, 24 Mill Road, Newbourne, Woodbridge, Suffolk, IP12 4NP, GB, GB (Residence), GB (Nationality), (Designated only for: US)
KING John Robert, 2 Hertfords Place, Chillesford, Woodbridge, Suffolk IP12 3SD, GB, GB (Residence), GB (Nationality), (Designated only for: US)
PATTERSON John, The Annexe, 5 The Mills, Playford Road, Rushmere St Andrew, Ipswich, Suffolk, IP4 5RL, GB, GB (Residence), GB (Nationality), (Designated only for: US)
Legal Representative:
SEMOS Robert Ernest Vickers (agent), BT Group Legal Services, Intellectual Property Dept., Holborn Centre, 8th floor, 120 Holborn, London EC1N 2TE, GB,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200122664 A1 20010329 (WO 0122664)
Application: WO 2000GB3678 20000925 (PCT/WO GB0003678)
Priority Application: GB 99307550 19990924
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/46
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 7751

English Abstract
A method of establishing a tunnel across an IPv4 domain for the transport of packets from a source host on one IPv6 domain to a destination host on another IPv6 domain, there being respective interfaces between the IPv4 domain and the IPv6 domains. The source host sends a normal IPv6 address request to its local DNS server, which relays it to an IPv6 name server in the other IPv6 domain. The response message, containing the true IPv6 address of the destination is received at the remote interface, which appends to the resulting protocol converted DNS response message a first

additional record containing the true IPv6 address, and a second additional record containing the IPv4 address of that interface. Upon receipt at the near interface, the additional records are stripped off, their contents stored in an entry of a table, and the true IPv6 address written into the address record of the resulting IPv6 DNS response message. When the near interface receives a packet from an IPv6 host, it checks whether the destination address matches an entry of its table, and if so sends the packet to the encapsulator together with the IPv4 address of the remote interface. The remote interface extracts the source address and the address of the encapsulating interface and stores these in an entry in its corresponding table for use in encapsulating return packets to the source. If, however, the destination address is recognised as being of IPv4-compatible or IPv4-mapped format, the packet is sent to a protocol converter.

French Abstract

L'invention concerne un procede d'etablissement d'un tunnel a travers un domaine de protocole IPv4 destine au transport de paquets d'un hote de source dans un domaine IPv6 a un hote de destination dans un autre domaine IPv6, des interfaces respectives existants entre le domaine IPv4 et les domaines IPv6. L'hote de source envoie une demande d'adresse Ipv6 normale a son serveur local de systeme de nom de domaines (DNS) qui le relaie vers un serveur de nom de protocole IPv6 dans l'autre domaine du protocole IPv6. Le message de reponse renfermant la veritable adresse du protocole IPv6 de la destination est recu a l'interface a distance qui est jointe au message resultant de reponse DNS converti en protocole, un premier enregistrement supplementaire contenant la veritable adresse du protocole IPv6 et un second enregistrement supplementaire contenant l'adresse du protocole IPv4 de cette interface. Apres reception au niveau de l'interface proche, les enregistrements supplementaires sont enleves, leurs contenus sont stockes dans une entree d'une table et la veritable adresse du protocole IPv6 inscrite dans l'enregistrement des adresses du message resultant de reponse DNS du protocole IPv6. Lorsque l'interface proche recoit un paquet d'un hote IPv6, elle verifie si l'adresse de destination correspond a une entree de sa table, et si tel est le cas, elle envoie le paquet a un encapsulateur conjointement a l'adresse du protocole IPv4 de l'interface a distance. Celle-ci extrait l'adresse de la source et l'adresse de l'interface d'encapsulage et les stocke dans une entree dans sa table correspondante utilisee pour encapsuler des paquets de retour vers la source. Si, toutefois, l'adresse de destination est reconnue comme etant compatible avec le protocole IPv4 ou de format IPv4, le paquet est envoye au convertisseur de protocole.

Legal Status (Type, Date, Text)

Publication 20010329 A1 With international search report.

Examination 20010621 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:

Detailed Description

Claims

Detailed Description

... deleted at midnight, when the day changes, or the address can be stored with a " **time** to **live** " value which is the start value of a count down timer. Similarly, the border router 1 6A deletes the entry in its IM/ **tunnel** endpoint table 76A after a short time. By preventing permanent storage of the address of...

Claim

... stored retrieved content, and rendering that stored retrieved content unuseable upon the expiry of the **time** to **live** .

8 A method as claimed in claim 7, wherein the rendering step deletes the stored retrieved content.

9 A method of establishing a **tunnel** from a first interface between a first network and a second network to a second...

9/5,K/23 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00554782 **Image available**

IP MOBILITY MECHANISM FOR A PACKET RADIO NETWORK

AGENCEMENT FOURNISSANT UNE MOBILITE PI A UNE STATION MOBILE

Patent Applicant/Assignee:
NOKIA NETWORKS OY,
VERKAMA Markku,
FLYKT Patrik,
HAUMONT Serge,
Inventor(s):
VERKAMA Markku,
FLYKT Patrik,
HAUMONT Serge,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200018155 A2 20000330 (WO 0018155)
Application: WO 99FI774 19990920 (PCT/WO FI9900774)
Priority Application: FI 982027 19980921
Designated States: AE AL AM AT AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ CZ DE DE DK DK DM EE EE ES FI FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: H04Q-007/22
International Patent Class: H04L-029/06
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 3212

English Abstract

An arrangement for providing IP mobility for a mobile station (MS). The mobile station (MS) has a care-of-address (COA) for routing data packets when the MS is away from home. The arrangement comprises support nodes, called access nodes (SGSN), and gateway nodes (GGSN), and a foreign agent (FA) having an IP address. In order to save IP addresses and radio resources the foreign agent (FA) is integrated into one of the support nodes (SGSN), and the IP address of, or provided by, the foreign agent (FA) is also used as the mobile station's (MS) care-of-address (COA).

French Abstract

Agencement fournissant une mobilite PI a une station mobile (SM). La station mobile (SM) presente une attention d'adresse (COA) pour l'acheminement des paquets de donnees lorsque la SM est hors de sa zone locale. L'agencement comprend des noeuds de prise en charge, appeles noeuds d'acces (SGSN), et des noeuds passerelle (GGSN), ainsi qu'un agent etranger (FA) ayant une adresse PI. Afin de sauvegarder les adresses PI et les ressources de radiocommunication, l'agent etranger (FA) est integre dans un des noeuds de prise en charge (SGSN), et l'adresse PI de, ou fournie par l'agent etranger (FA) est egalement utilisee comme attention d'adresse (COA) de la station mobile (SM).

Fulltext Availability:
Detailed Description

Detailed Description

... integration relates to the time-to-live field of IP datagrarns. IP datagrams comprise a **time** -to- **live** field which is decremented by one when the datagram is routed by a router or **tunnelled** by a host (or a GGSN) to a new destination. (The **time** -to- **live** field is also called a hop count or a hop limit.) There are two mechanisms...

File 347:JAPIO Nov 1976-2003/Nov(Updated 040308)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200417
(c) 2004 Thomson Derwent

Set	Items	Description
S1	4385	TTL OR TTF OR TIME(1W)(LIVE OR LIFE)
S2	96	(HOP OR HOPS)(2N)(LIMIT??? ? OR LIMITATION? OR COUNT??? ? - OR ALLOW?)
S3	498	(IP OR INTERNET OR PROTOCOL OR ICMP OR DNS)(1W)(FIELD? ? OR HEADER? ?)
S4	66923	TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S5	165	IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5 OR SOCKS(-)V5 OR LAYER()(TWO OR 2)()FORWARD??? ? OR L2F
S6	1142	VPN OR VPNS OR VIRTUAL()PRIVATE()(NET OR NETWORK? ?)
S7	928851	ENCAPSULAT? OR WRAP???? ? OR INSULAT?
S8	14649	(SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHER?)(2N)(CONNECT???? ? OR CONNECTIVIT? OR CHANNEL? ? OR PATH? ? OR PATHWAY? OR PASSAGE? ?)
S9	8026	(SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHER?)(2N)(COMMUNICAT???? ? OR ACCESS OR ACCESS?? ? OR ACCESSING)
S10	2562	PRIVATE(1W)(NET OR NETS OR NETWORK?)
S11	1172182	VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALIDAT? OR CHECK??? ? OR CHEQU? OR EXAMIN? OR TEST OR TESTS OR TESTED OR TESTING? OR EVALUAT? OR CONFIRM?
S12	22359	AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CROSSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQU?
S13	140	S1:S3 AND S4:S10
S14	21	S13 AND S11:S12
S15	21	IDPAT (sorted in duplicate/non-duplicate order)
S16	21	IDPAT (primary/non-duplicate records only)

16/9/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015903518 **Image available**
WPI Acc No: 2004-061358/200406
Related WPI Acc No: 2004-061351; 2004-061365; 2004-061367
XRPX Acc No: N04-049721

Data structure for gateway computer, has security parameters index field associated with non-local address field, to store security parameters index associated with communication from remote non-local device

Patent Assignee: NVIDIA CORP (NVID-N)
Inventor: MAUFER T A; NANDA S; SIDENBLAD P J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030233475	A1	20031218	US 2002172046	A	20020613	200406	B

Priority Applications (No Type Date): US 2002172046 A 20020613
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030233475	A1		20	G06F-015/16	

Abstract (Basic): US 20030233475 A1
NOVELTY - The structure has medium access control address field associated with local and non-local public address fields, and a security parameters index field associated with non-local address field. The index field storing parameter index associated with

non-local device, is associated with security **protocol field** storing security protocol number selected from **authentication** header (AH) and **encapsulating** security bag load.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) method for network translation (NAT) protocol integration with **authentication** header (AH) protected packet;

(2) mapping table generation method;

(3) packet formation method; and

(4) signal bearing medium storing data packet forming program.

USE - Data structure for gateway computer e.g. network address translation (NAT) gateway computer for integration with internet protocol security (**IPSec**).

ADVANTAGE - Enhances **security** for data **communications** over the network. Enables to integrate NAT and **IPSec** without adding overhead and without requiring an identification source or destination address. Enables to form packets without using a private IP address. and public identification address provided by NAT device.

DESCRIPTION OF DRAWING(S) - The figure shows a flow chart explaining the integration method of NAT with **IPSec** protected packet.

pp; 20 DwgNo 3/5

Title Terms: DATA; STRUCTURE; GATEWAY; COMPUTER; SECURE; PARAMETER; INDEX; FIELD; ASSOCIATE; NON; LOCAL; ADDRESS; FIELD; STORAGE; SECURE; PARAMETER; INDEX; ASSOCIATE; COMMUNICATE; REMOTE; NON; LOCAL; DEVICE

Derwent Class: T01; W01

International Patent Class (Main): G06F-015/16

File Segment: EPI

Manual Codes (EPI/S-X): T01-N02B1; T01-S03; W01-A03B; W01-A06F; W01-A06G2

16/9/2 (Item 2 from file: 350)

DIALOG(R)File 350:Derwent WPIX

015749407 **Image available**

WPI Acc No: 2003-811608/200376

XRPX Acc No: N03-649806

Data acquisition method in Internet, involves supplying data packet to client application, if header of Internet protocol frame comprising packet is valid

Patent Assignee: LOCKWOOD J W (LOCK-I); SCHUEHLER D V (SCHU-I)

Inventor: LOCKWOOD J W; SCHUEHLER D V

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20030177253	A1	20030918	US 2002222307	A	20020815	200376 B

Priority Applications (No Type Date): US 2002222307 A 20020815

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030177253	A1		15	G06F-015/16	

Abstract (Basic): US 20030177253 A1

NOVELTY - An Internet **protocol** (**IP**) **header** (18) and a data packet are removed from an IP frame (12) received in a transmission control protocol (TCP) splitter (10) placed between source and destination devices (14,16). If the **checksum** of the header is invalid, the IP frame is dropped and accumulated in the TCP splitter. Else, a client application (20) is supplied with the data packet and

the IP frame is sent to the destination device, with removed header.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(1) apparatus for facilitating data transmission;
(2) network;
(3) method for identifying and selectively removing data; and
(4) dynamically reconfigurable data transmission system.
USE - For acquiring data through Internet, transmission control protocol (TCP) network.
ADVANTAGE - Enables effective monitoring of data with high bandwidth rates.
DESCRIPTION OF DRAWING(S) - The figure shows high level block diagram of the dataflow through the TCP splitter.
TCP splitter (10)
IP frames (12)
source device (14)
destination device (16)
IP header (18)
client application (20)
cell **wrapper** (24)
pp; 15 DwgNo 1/6
Title Terms: DATA; ACQUIRE; METHOD; SUPPLY; DATA; PACKET; CLIENT; APPLY; HEADER; PROTOCOL; FRAME; COMPRISE; PACKET; VALID
Derwent Class: T01; W01
International Patent Class (Main): G06F-015/16
File Segment: EPI
Manual Codes (EPI/S-X): T01-N02A1; T01-N02A3B; W01-A03B; W01-A06A; W01-A06E1; W01-A06F2C

16/9/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015747741 **Image available**
WPI Acc No: 2003-809942/200376
Method for protecting packet on improved ip layer providing multiple security service
Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N)
Inventor: NA J H; PARK S H; SON S W
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2003055715	A	20030704	KR 200185777	A	20011227	200376	B

Priority Applications (No Type Date): KR 200185777 A 20011227
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2003055715	A		1	G06F-015/16	

Abstract (Basic): KR 2003055715 A
NOVELTY - A method for protecting a packet on an improved IP(Internet Protocol) layer providing a multiple security service is provided to offer a multiple information protection service for each packet on the IP layer that is independently realized and operated without influencing on an application layer service program.
DETAILED DESCRIPTION - After generating an **IP header** of the packet to transmit, the packet security service is selected by referring to a security policy database and a security linked database(S107). A process for **encapsulation** , padding, encryption process, ICV(Integrity **Check** Value) calculation, and serial number

value generation is performed according to respective service sorts by judging that the sort of the security service is the AH(**Authentication** Header) or the ESP(**Encapsulating** Security Payload)(S138-S128, S132-S122). A **tunneling** /transport header is generated and transferred to an IP packet fragmentation function(S130,S124). In order to provide the multiple security service, three steps are repeatedly carried out.

pp; 1 DwgNo 1/10

Title Terms: METHOD; PROTECT; PACKET; IMPROVE; IP; LAYER; MULTIPLE; SECURE; SERVICE

Derwent Class: T01

International Patent Class (Main): G06F-015/16

File Segment: EPI

Manual Codes (EPI/S-X): T01-M02

16/9/4 (Item 4 from file: 350)

015624047 **Image available**

WPI Acc No: 2003-686218/200365

Method for receiving L2TP **packet at high speed to improve LNS performance of** VPN **router**

Patent Assignee: LG ELECTRONICS INC (GLDS)

Inventor: PARK J H

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2003033558	A	20030501	KR 200165587	A	20011024	200365	B

Priority Applications (No Type Date): KR 200165587 A 20011024

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2003033558	A		1	H04L-012/56	

Abstract (Basic): KR 2003033558 A

NOVELTY - A method for receiving an **L2TP** (Layer 2 **Tunneling** Protocol) packet at high speed to improve LNS (**L2TP** Network Server) performance of a **VPN** (**Virtual Private Network**) router is provided to allow an LSL (Link Support Layer) block to analyze a header of the **L2TP** packet and interpret **tunnel** ID and call ID information, to transmit the information directly to a virtual serial device driver block for processing by a PPP (Point-to-Point Protocol) server, so as to reduce overheads.

DETAILED DESCRIPTION - If a packet is received to an LSL block (S101), whether the provision of an LNS function of a **VPN** router is available is decided (S102). If so, a pipe filter receives the packet and whether the packet is an IP (Internet Protocol) packet is **checked** (S103). If so, whether an IP payload is a UDP (User Datagram Protocol) packet is **checked** (S104). If so, whether the packet is an **L2TP** packet is **checked** (S105). If so, whether the packet is a data packet is **checked** (S106). If so, whether flow control is applied to the data packet is decided (S107). If above filtering conditions are all met, an **L2TP** header of the received packet is analyzed, to interpret a **tunnel** ID and a call ID (S108). An **IP header** , a UDP header and the **L2TP** header are eliminated (S109). The packet is delivered to an API (Application Program Interface) of a virtual serial device driver to process the packet (S110,S111). And if any filtering condition is not met, an existing packet processing method is used to process the packet (S112).

pp; 1 DwgNo 1/10
Title Terms: METHOD; RECEIVE; PACKET; HIGH; SPEED; IMPROVE; PERFORMANCE; ROUTER
Derwent Class: T01; W01
International Patent Class (Main): H04L-012/56
File Segment: EPI
Manual Codes (EPI/S-X): T01-N02A1; T01-N02A2; T01-N02B; W01-A03B; W01-A06F3; W01-A06F9; W01-A06G2

16/9/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015193532 **Image available**
WPI Acc No: 2003-254066/200325
Internet protocol (IP) packet transmission method for protection IP packet in which encryption and authentication **information is added in the received packet**
Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N)
Inventor: JUNG J H; LEE J T; PARK S H
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2002088728	A	20021129	KR 200127614	A	20010521	200325	B

Priority Applications (No Type Date): KR 200127614 A 20010521
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2002088728	A		1	H04L-012/56	

Abstract (Basic): KR 2002088728 A

NOVELTY - A transmission host terminal receives a packet from an application layer(601), and generates an information protection packet in which encryption and **authentication** information is added in the received packet(602). A data link header is added in the generated information protection packet, and the added information protection packet is transmitted to a gateway through the Internet by a frame unit(603). The gateway receives the transmitted information protection packet, removes the data link header from the received information protection packet, and forwards the removed information protection packet(604,605).

DETAILED DESCRIPTION - In case that a security service is selected, the information protection packet is encoded and decoded according to an AH(**Authentication** Header) **protocol header** and an ESP(**Encapsulating** Security Payload) **protocol header** , and an information protection packet in which a data link header is added again is transmitted to the Internet(606). A reception host terminal receives the information protection packet forwarded from the gateway, and deletes the data link header from the received information protection packet(607). The reception host terminal **checks authentication** data according to the selection of the security service, and **confirms** decoding and **authentication** information according to the AH **protocol header** and the ESP **protocol header** (608). The reception host terminal transmits the received data to the upper application layer(609).

ADVANTAGE - A method for transmitting and receiving an information protection IP(Internet Protocol) packet is provided to generate and transmit a security packet in an IP layer without having an influence on an application layer service program.

pp; 1 DwgNo 1/10
Title Terms: PROTOCOL; IP; PACKET; TRANSMISSION; METHOD; PROTECT; IP; PACKET; ENCRYPTION; AUTHENTICITY; INFORMATION; ADD; RECEIVE; PACKET
Derwent Class: T01; W01
International Patent Class (Main): H04L-012/56
File Segment: EPI
Manual Codes (EPI/S-X): T01-D01; T01-N01D; W01-A03B; W01-A05A; W01-A06F2A; W01-A06G2

16/9/6 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014992467 **Image available**
WPI Acc No: 2004-180869/200417
XRPX Acc No: N04-143799
Network node authentication **process for wireless computer network, involves exchanging access control parameters that define network nodes ability to access other resources accessible through computer network**
Patent Assignee: WIRELESS SECURITY CORP (WIRE-N)
Inventor: BRUESTLE J J; LILLIE T L
Number of Countries: 104 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200415958	A2	20040219	WO 2003US25420	A	20030812	200417	B

Priority Applications (No Type Date): US 2002403104 P 20020812
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200415958	A2	E	18	H04L-029/06	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW

Abstract (Basic): WO 200415958 A2
NOVELTY - The process involves exchanging access control parameters that define network nodes ability to access other resources through a computer network. The parameters are provided by an **authentication** server (16) e.g. RADIUS server, to an access point via which the network node seeks to gain access to the computer network. The process requires the identification of the node and the server to one another using digital certificates.
USE - Used for providing network node **authentication** in a wireless computer network that utilizes EAP TTLS, EAP TLS, Protected EAP Protocol (PEAP) or other **authentication** procedures.
ADVANTAGE - The method enhances network security and permits greater control over client access to network resources.
DESCRIPTION OF DRAWING(S) - The drawing shows an extensible **authentication** protocol (EAP) **tunneled** transport layer security (TTLS) **authentication** exchange between a client, an access point, a TTLS server and an **authentication** server.
Access point (12)
TTL server (14)
Authentication server (16)

Messages (116,122)
pp; 18 DwgNo 2/3
Title Terms: NETWORK; NODE; AUTHENTICITY; PROCESS; WIRELESS; COMPUTER; NETWORK; EXCHANGE; ACCESS; CONTROL; PARAMETER; DEFINE; NETWORK; NODE; ABILITY; ACCESS; RESOURCE; ACCESS; THROUGH; COMPUTER; NETWORK
Derwent Class: T01; W01
International Patent Class (Main): H04L-029/06
File Segment: EPI
Manual Codes (EPI/S-X): T01-N02A1; T01-N02A3B; T01-N02B1; W01-A05B; W01-A07G; W01-B05A

16/9/7 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014952396 **Image available**
WPI Acc No: 2003-012909/200301
Method for enhancing transmission speed using hop count **in mobile computing environment**
Patent Assignee: LG ELECTRONICS INC (GLDS)
Inventor: PARK B B
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2002052066	A	20020702	KR 200081248	A	20001223	200301	B

Priority Applications (No Type Date): KR 200081248 A 20001223
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2002052066	A		1	H04L-012/56	

Abstract (Basic): KR 2002052066 A
NOVELTY - A method for enhancing transmission speed using **hop count** in mobile computing environment is provided to use a **hop count** module to a reception function of a transmission protocol, thereby achieving a routing optimization at the optimum **hop count** .
DETAILED DESCRIPTION - A **hop count** for providing the optimum transmission capability according to a time of movement is set to a transmission control protocol of a mobile host(MH)(S10). Thereafter, position information of MH and data at a transmitter, as a Correspondent Host(CA), is transmitted to a home agent(HA)(S11). The HA receives the data, **check** the position of the MH and then discriminates whether the MH belongs to a charge region of HA(S12). If the MH belongs to a charge region of HA, the HA transmits data to the MH. The MH receives the data and discriminates whether the **hop count** is the same as a time of movement(S13). If the **hop count** is not the same as a time of movement, the MH transmits a response message to the received message to the HA(S14). The HA transmits the message to the CA(S15). The CA **checks** the message from the HA and **confirms** whether a conversion message exists via a route optimum method(S16). If the **hop count** is the same as a time of movement, the MH transmits a conversion message to the HA and a foreign agent(FA)(S17). The HA and FA transmit a response message to the CA(S18). If the conversion message is **confirmed** , the CA transmits data to the HA(S19). The data of CA is transmitted to the MH by the HA, the discrimination of sameness between the **hop count** and a time of movement is performed(S20). If it is discriminated that the position of MH do not belong to the charge region, the HA performs a **tunneling** to the FA. Thereafter, the FA transmits the data received from the CA to MH(S21).

pp; 1 DwgNo 1/10
Title Terms: METHOD; ENHANCE; TRANSMISSION; SPEED; HOP; COUNT; MOBILE; COMPUTATION; ENVIRONMENT
Derwent Class: W01
International Patent Class (Main): H04L-012/56
File Segment: EPI
Manual Codes (EPI/S-X): W01-A03B; W01-A06G2

16/9/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014952126 **Image available**
WPI Acc No: 2003-012639/200301
Method for creating pdp context in gprs network
Patent Assignee: LG ELECTRONICS INC (GLDS)
Inventor: HONG J M
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2002051559	A	20020629	KR 200080932	A	20001222	200301	B

Priority Applications (No Type Date): KR 200080932 A 20001222
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2002051559	A		1	H04L-012/56	

Abstract (Basic): KR 2002051559 A
NOVELTY - A method for creating a PDP(Packet Data Protocol) context in a GPRS(General Packet Radio Service) network is provided to select and use a GRE(Generic Routing **Encapsulation**) protocol, other than a GTP-U protocol, as a user traffic protocol by adding a traffic **protocol field** to a create PDP context request message in creating a PDP context for the **tunnel** allocation between an SGSN(Serving GPRS Support Node) and a GGSN(Gateway GSN).
DETAILED DESCRIPTION - An SGSN adds a traffic **protocol field** to select a user traffic protocol to a create PDP context request message and transmits it to a GGSN(S51). Receiving the create PDP context request message(S52), the GGSN **checks** the traffic **protocol field** value of the message and **confirms** whether it indicates a GTP-U protocol or a GRE protocol(S53). In case that the traffic **protocol field** value is '1', the GGSN selects the GTP-U protocol as the user traffic protocol(S54), allocates its own TEID value to the TEID field of a create PDP context response message, and transmits the response message to the SGSN(S55). However. if the traffic **protocol field** value is '2', the GGSN selects the GRE protocol(S56), writes a GRE key value, provided by the SGSN, in the TEID field of the create PDP context response message, and transmits the response message to the SGSN(S57).
pp; 1 DwgNo 1/10
Title Terms: METHOD; CONTEXT; NETWORK
Derwent Class: W01
International Patent Class (Main): H04L-012/56
File Segment: EPI
Manual Codes (EPI/S-X): W01-A03B; W01-A06G2

16/9/9 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014794824 **Image available**
WPI Acc No: 2002-615530/200266

System for constructing virtual multicast network

Patent Assignee: ZOOINNET (ZOOI-N); EGC & C LTD (EGCC-N)
Inventor: PARK H J; KIM Y; PARK H
Number of Countries: 100 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2002023100	A	20020328	KR 200129308	A	20010528	200266	B
WO 200298063	A1	20021205	WO 2002KR1003	A	20020528	200306	

Priority Applications (No Type Date): KR 200129308 A 20010528
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2002023100	A		1	H04L-012/28	
WO 200298063	A1	E		H04L-012/28	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

Abstract (Basic): KR 2002023100 A

NOVELTY - A system for constructing a virtual multicast network is provided to comprise a multicast agent installed in a user PC as well as a virtual multicast router having a multicast router function on a network, and to comprise a multicast management server for managing information on each virtual multicast router, so as to use a multicast service under non-multicast environments.

DETAILED DESCRIPTION - A virtual multicast router(30) performs a dynamic **tunneling** for data transceiving between the virtual multicast router(30) and other virtual multicast router/multicast agent, by using an IP **tunneling** /UDP(User Datagram Protocol) **tunneling** , and manages multicast membership information of the other virtual multicast router and multicast agents. The virtual multicast router(30) transmits multicast data to a multicast agent and other virtual multicast router participating in a specific multicast group, and transmits multicast data between virtual multicast routers. The virtual multicast router(30) **checks** whether a multicast router exists in a self sub network. If so, the virtual multicast router(30) plays a role of multicast repeater only. A multicast agent(52) uses a dynamic **tunneling** for multicast data transceiving with the virtual multicast router(30), and uses a UDP **tunneling** for the dynamic **tunneling** , then retransmits the data of the virtual multicast router(30) to a multicast application program. The multicast agent(52) limits to **TTL** (**Time** to **Live**) 0 by using an IP multicast while re-transmitting the data, to perform a re-multicast for an operating computer only. A multicast management server(20) performs an IP caching for the multicast agent(52) that requests a retrieval and the retrieved virtual multicast router(30), and performs a caching for the multicast agent(52) or an IP address of the virtual multicast router(30), and a network address as well as the multicast agent(52), an IP address of the nearest virtual multicast router retrieved by the virtual multicast router(30), and the network address.

pp; 1 DwgNo 1/10

Title Terms: SYSTEM; CONSTRUCTION; VIRTUAL; NETWORK
Derwent Class: W01

International Patent Class (Main): H04L-012/28
File Segment: EPI
Manual Codes (EPI/S-X): W01-A06

16/9/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014447909 **Image available**
WPI Acc No: 2002-268612/200231
XRPX Acc No: N02-209064
Network address translation system for accessing Internet, has private network **router which translates globally unique IP address into corresponding non-globally unique IP address**
Patent Assignee: AT & T WIRELESS SERVICES INC (AMTT)
Inventor: HARRANG J P
Number of Countries: 026 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200197485	A2	20011220	WO 2001US14765	A	20010508	200231	B
TW 538616	A	20030621	TW 2001113964	A	20010608	200377	

Priority Applications (No Type Date): US 2000724774 A 20001128; US 2000211497 P 20000614
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200197485	A2	E	40	H04L-029/12	

Designated States (National): BR CA CN ID IN JP
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

TW 538616	A		H04L-029/12

Abstract (Basic): WO 200197485 A2
NOVELTY - A **private network** router (20) performs network address translation of non-globally unique IP address to a globally unique IP address. Another **private network** router (30) performs network translation of the globally unique IP address to the corresponding non-globally unique IP address.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for computer program product.
USE - For translating globally unique IP address into non-globally unique IP address, for accessing Internet using PC, PDA, smart pages, cellular telephones, etc.
ADVANTAGE - Eliminates the need for additional bandwidth. Facilitates orderly topology-based routing to the computer through the **private** address **networks** . Eliminates the need for inspection and possible modification of IP datagram payload, when translating addresses in **IP** datagram **header** . Allows arbitrary end-to-end IP datagram encryption and **authentication** arrangements to inter-operate between public networks.
DESCRIPTION OF DRAWING(S) - The figure shows the sketch of the local network connected to a **private network** .
Private network routers (20,30)
pp; 40 DwgNo 1/6
Title Terms: NETWORK; ADDRESS; TRANSLATION; SYSTEM; ACCESS; PRIVATE; NETWORK; ROUTER; TRANSLATION; UNIQUE; IP; ADDRESS; CORRESPOND; NON; UNIQUE; IP; ADDRESS
Derwent Class: T01; W01
International Patent Class (Main): H04L-029/12

File Segment: EPI
Manual Codes (EPI/S-X): T01-M06A1A; T01-N02A3B; T01-N02B1B; T01-S03;
W01-A06F2A; W01-C01D3C

16/9/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014316963 **Image available**
WPI Acc No: 2002-137665/200218
Fading process method of ppp frame in virtual private network
Patent Assignee: SAMSUNG ELECTRONICS CO LTD (SMSU)
Inventor: PARK H J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2001084657	A	20010906	KR 20009852	A	20000228	200218	B

Priority Applications (No Type Date): KR 20009852 A 20000228
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2001084657	A		1	H04L-012/56	

Abstract (Basic): KR 2001084657 A
NOVELTY - A fading process method of a PPP(Point-to-Point Protocol) frame in a **virtual private network** (**VPN**) is provided to accurately recognize the PPP frame in a remote PC by performing the fading process of a data field which is more than an acceptable frame distance in a PPP stack of the remote PC among the PPP frame to remove the data field and transmitting the PPP frame to the remote PC.
DETAILED DESCRIPTION - If a **PPTP** (PPP **Tunneling** Protocol) frame is received from a PNS(**PPTP** Network Service) server of a **VPN** (300), an RAS(Remote Access Service) perform a decapsulation process of an **IP header** and a GRE header from the **PPTP** frame and removes the **IP header** and the GRE header(302). The RAS **checks** a distance of a PPP frame from a PPP frame header(304). The RAS **checks** whether a data field which is more than an acceptable frame length in a remote PC among the PPP frame exists(306). If the data field which is more than the acceptable frame length in the remote PC exists, the RAS performs a fading process of the data field and removes the data field from the PPP frame(308). The RAS **checks** whether the remote PC is connected through a PSTN(Public Switched Telephone Network) or an ISDN(Integrated Service Digital Network)(310). If the remote PC is connected through the PSTN, the RAS processes the PPP frame in which the data field is removed as an asynchronous frame and transmits the processed PPP frame to the remote PC(312). If the remote PC is connected through the ISDN, the RAS transmits the PPP frame to the remote PC(314).
Dwg.1/10
Title Terms: FADE; PROCESS; METHOD; FRAME; VIRTUAL; PRIVATE; NETWORK
Derwent Class: W01
International Patent Class (Main): H04L-012/56
File Segment: EPI
Manual Codes (EPI/S-X): W01-A03B; W01-A06G2

16/9/12 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014037772 **Image available**
WPI Acc No: 2001-521985/200157
XRPX Acc No: N01-386874

Scheme for determining transport level information in the presence of Internet protocol security encryption using the header to record unencrypted information normally included in the payload

Patent Assignee: KOODLI R (KOOD-I); NOKIA CORP (OYNO); SENGODAN S (SENG-I)
Inventor: KOODLI R; SENGODAN S

Number of Countries: 093 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200147169	A2	20010628	WO 2000US34991	A	20001226	200157	B
AU 200132659	A	20010703	AU 200132659	A	20001226	200164	
EP 1240766	A2	20020918	EP 2000991431	A	20001226	200269	
			WO 2000US34991	A	20001226		
EP 1240766	B1	20030820	EP 2000991431	A	20001226	200356	
			WO 2000US34991	A	20001226		
DE 60004707	E	20030925	DE 604707	A	20001226	200371	
			EP 2000991431	A	20001226		
			WO 2000US34991	A	20001226		

Priority Applications (No Type Date): US 99471083 A 19991223
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200147169	A2	E	19	H04L-000/00	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW				
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW					
AU 200132659	A			H04L-000/00	Based on patent WO 200147169
EP 1240766	A2	E		H04L-029/06	Based on patent WO 200147169
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
EP 1240766	B1	E		H04L-029/06	Based on patent WO 200147169
Designated States (Regional): DE FR GB IT					
DE 60004707	E			H04L-029/06	Based on patent EP 1240766
					Based on patent WO 200147169

Abstract (Basic): WO 200147169 A2

NOVELTY - A transport payload data unit (106) and an **encapsulated** security payload (ESP) trailer (108) are fully encrypted whereas the **Internet protocol header** (102), the ESP header (104) and the ESP **authenticator** (110) are not encrypted. Some information related to the selected information is placed in the security **protocol header** prior to security processing of the packet, so that access can be allowed to selected information by intermediate nodes during transmission of the packet.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for a method of permitting access to selected information in an encrypted packet.

USE - Determining transport level information in presence of Internet protocol security encryption.

ADVANTAGE - No compromise of security.

DESCRIPTION OF DRAWING(S) - The drawing is a schematic diagram of configuration of an Internet protocol packet

Payload data unit (106)
ESP trailer (108)
Internet protocol header (102)
ESP header (104)

pp; 19 DwgNo 1/5
Title Terms: SCHEME; DETERMINE; TRANSPORT; LEVEL; INFORMATION; PRESENCE; PROTOCOL; SECURE; ENCRYPTION; HEADER; RECORD; INFORMATION; NORMAL; PAYLOAD
Derwent Class: T01; W01
International Patent Class (Main): H04L-000/00; H04L-029/06
File Segment: EPI
Manual Codes (EPI/S-X): T01-D01; W01-A03B; W01-A05A; W01-A06B7; W01-A06F; W01-A06G2

16/9/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013941179 **Image available**
WPI Acc No: 2001-425393/200145
XRPX Acc No: N01-315619
Secure address resolution for private network **constructed on public network e.g. internet infrastructure which relieves burdens on network administrator**
Patent Assignee: SUN MICROSYSTEMS INC (SUNM)
Inventor: CARONNI G; GUPTA A; KUMAR S; MARKSON T R; SCHUBA C L; SCOTT G C
Number of Countries: 093 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200143391	A2	20010614	WO 2000US33458	A	20001211	200145	B
AU 200120810	A	20010618	AU 200120810	A	20001211	200161	

Priority Applications (No Type Date): US 99457894 A 19991210
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200143391	A2	E	33	H04L-029/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200120810	A		H04L-029/00	Based on patent WO 200143391

Abstract (Basic): WO 200143391 A2
NOVELTY - A **private network** 'Supernet', runs on a public-network infrastructure. A program in the Supernet creates address mappings, this program is **authenticated** to ensure that it can be trusted and will not violate the integrity of the system. The address mappings have an associated **time** -to- **live** (**TTL**), which indicates an expiration time, upon which the mappings become invalid.
USE - Provide secure address resolution for a **private network** .
ADVANTAGE - Relieves management burden on network administrator.
DESCRIPTION OF DRAWING(S) - The drawing shows the Supernet structure.
pp; 33 DwgNo 3/10
Title Terms: SECURE; ADDRESS; RESOLUTION; PRIVATE; NETWORK; CONSTRUCTION; PUBLIC; NETWORK; RELIEVE; NETWORK; ADMINISTER
Derwent Class: W01
International Patent Class (Main): H04L-029/00
File Segment: EPI
Manual Codes (EPI/S-X): W01-A06E1; W01-A06G3

16/9/14 (Item 14 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012066452 **Image available**
WPI Acc No: 1998-483363/199842
XRPX Acc No: N98-377128

Asynchronous transfer mode network for ensuring security **of** communication **- has packet filtering function; transmits signalling message, containing source and destination network-layer and transport-layer addresses, from source node to network**

Patent Assignee: NEC CORP (NIDE)
Inventor: MORI N
Number of Countries: 027 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 866630	A1	19980923	EP 98301110	A	19980216	199842	B
JP 10229401	A	19980825	JP 9730436	A	19970214	199844	
CA 2229652	A	19980814	CA 2229652	A	19980216	199901	
JP 11032047	A	19990202	JP 97183665	A	19970709	199915	
JP 3000968	B2	20000117	JP 97183665	A	19970709	200008	
US 6172991	B1	20010109	US 9824101	A	19980217	200104	
CA 2229652	C	20020521	CA 2229652	A	19980216	200248	

Priority Applications (No Type Date): JP 97183665 A 19970709; JP 9730436 A 19970214
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 866630	A1	E	28	H04Q-011/00	
Designated States (Regional): AL AT BE CH DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
JP 10229401	A		13	H04L-012/28	
CA 2229652	A			H04L-012/56	
JP 11032047	A		16	H04L-012/28	
JP 3000968	B2		16	H04L-012/28	Previous Publ. patent JP 11032047
US 6172991	B1			H04L-012/28	
CA 2229652	C	E		H04L-012/56	

Abstract (Basic): EP 866630 A

The communication system receives packets at a source node and transmits a signalling message containing source and destination, network-layer and transport-layer addresses of the packet to the network. The source node has a virtual connection management table, and the ATM network has a filtering table (33), with entries storing source and destination addresses. The ATM network transmits a grant indication message to the source node if the contents of the received signalling message are identical to one of it's filtering table entries; and a virtual connection is set up.

The source node responds to the grant indication message by storing the packet's addresses in it's virtual connection management table. Subsequently received packets are segmented into cells, and the cells are transmitted over the virtual connection, if the packet contains addresses identical to the addresses stored in the virtual connection management table.

USE - **Secure** Internet **communication** using transmission control protocol/Internet protocol (TCP/IP) over ATM network.

ADVANTAGE - Provides security function in high speed ATM switch, where previously transit switches did not **check** third and fourth layer TCP/ **IP headers**

Dwg.2/16

Title Terms: ASYNCHRONOUS; TRANSFER; MODE; NETWORK; ENSURE; SECURE;

COMMUNICATE; PACKET; FILTER; FUNCTION; TRANSMIT; SIGNAL; MESSAGE; CONTAIN ; SOURCE; DESTINATION; NETWORK; LAYER; TRANSPORT; LAYER; ADDRESS; SOURCE; NODE; NETWORK
Derwent Class: W01
International Patent Class (Main): H04L-012/28; H04L-012/56; H04Q-011/00
International Patent Class (Additional): H04L-012/46; H04L-029/04; H04L-029/08; H04Q-003/00
File Segment: EPI
Manual Codes (EPI/S-X): W01-A03B1; W01-A06E1; W01-A06F; W01-A06G2; W01-B07

16/9/15 (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008075047
WPI Acc No: 1989-340159/198946
XRPX Acc No: N89-258928
Data communication **system for** security **network - uses slave transponders and master nodes acting under accordion-like protocol which can conform to message transmitted**
Patent Assignee: VINDICATOR CORP (VIND-N); VINDICATOR (VIND-N); VINDICATOR (VINI-N)
Inventor: SKRET D L
Number of Countries: 004 Number of Patents: 010
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 8910666	A	19891102				198946 B
AU 8935611	A	19891124				199016
US 4980913	A	19901225	US 88183112	A	19880419	199103
EP 413737	A	19910227	EP 89905488	A	19890418	199109
US 5001755	A	19910319	US 90497052	A	19900321	199114
JP 3505149	W	19911107	JP 90505241	A	19900418	199151
AU 9227102	A	19921217	AU 9227102	A	19921016	199306
			AU 8935611	A	19890000	
AU 644765	B	19931216	AU 9227102	A	19921016	199406
			AU 8935611	A	19890000	
EP 413737	A4	19930728	EP 89905488	A	19890000	199527
KR 9411489	B1	19941219	WO 89US1620	A	19890418	199643
			KR 89702392	A	19891219	

Priority Applications (No Type Date): US 88183112 A 19880419; US 90497052 A 19900321
Cited Patents: US 4679189; US 4768190; US 4787082; 4.Jnl.Ref; US 4145568; US 4316055; US 4654480
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 8910666	A	E	7		
AU 9227102	A			H04L-009/00	Div ex application AU 8935611
AU 644765	B			H04L-009/00	Div ex application AU 8935611 Previous Publ. patent AU 9227102
KR 9411489	B1			H04L-009/00	

Abstract (Basic): WO 8910666 A
A series of slave transponders (T) are coupled, via a full duplex bus, to a master node (GW), which is itself coupled to other nodes network. forming a The Master node periodically polls the slave transponders.. to **authenticate** them and directs transmission to appropriate end point.
The system employs an accordion-like protocol conforming to the transmitted message, the protocol beings with address bytes, followed

by control field identifying the fields present, and is data transparent. The sequence field allows protocol to handle both redundant and non-redundant lines.

USE/ADVANTAGE - Data **communication** system for **security** network. (37pp' Dwg.No.1/3)

Abstract (Equivalent): US 5001755 A

The data transmission encrypting method involves generating an identical sequence of pseudorandom numbers at both a transmitting and a receiving node. A key identifying a starting position in the sequence is provided to both transmitting and receiving nodes. The position in the sequence is incremented at both transmitting and receiving nodes for each predetermined portion of data transmission between the nodes.

Segments of the data transmissions are encrypted using pseudorandom numbers using the starting position for a first segment corresp. to the first position and using subsequent numbers for succeeding segments corresp. to succeeding portions. The whole process is repeated for each pair of nodes such that each node uses a different sequence position for each node it communicates with. (11pp)

US 4980913 A

The security system has a series of slave transponders coupled via a full duplex bus to a master node. The master node is coupled to other master nodes to form a network. The master node periodically polls its slave transponders to **authenticate** them. Each transponder has processing capability to give a distributed processing system. Each master node is a gateway which directs transmissions to the appropriate end point.

The system uses an accordion-like protocol which can have fields added or deleted in a specific structure to conform the protocol to the particular message being transmitted. The protocol begins with address bytes identifying the destination followed by a control field which identifies the fields which are present. For a broadcast, rather than a point-to-point transmission, a process ID field in the protocol determines what area or function has to be addressed in all units. This area or function can be addressed for a large number of nodes by using this **protocol field** .

USE - In communication system. (12pp)g

Title Terms: DATA; COMMUNICATE; SYSTEM; SECURE; NETWORK; SLAVE; TRANSPONDER ; MASTER; NODE; ACT; ACCORDION; PROTOCOL; CAN; CONFORM; MESSAGE; TRANSMIT

Derwent Class: W01; W05

International Patent Class (Additional): G08B-013/00; H04J-003/24; H04L-009/02; H04L-012/28

File Segment: EPI

Manual Codes (EPI/S-X): W01-A05; W01-A06B1; W01-A06C1; W05-B01; W05-B05

16/9/18 (Item 18 from file: 347)

DIALOG(R)File 347:JAPIO

07710430 **Image available**

COMMUNICATION SYSTEM, LAN CONTROLLER EQUIPPED WITH **ENCRYPTION** FUNCTION AND **COMMUNICATION** CONTROL PROGRAM

PUB. NO.: 2003-204326 [JP 2003204326 A]

PUBLISHED: July 18, 2003 (20030718)

INVENTOR(s): SAKAGUCHI TADAHIKO

APPLICANT(s): NEC CORP

APPL. NO.: 2002-002704 [JP 20022704]

FILED: January 09, 2002 (20020109)

INTL CLASS: H04L-009/36; H04L-012/22

ABSTRACT

PROBLEM TO BE SOLVED: To provide a communication system wherein important secret data is prevented from leaking by constructing a transmission packet such that it cannot be decoded with an apparatus operating on the basis of an ordinary IP-SEC specification, and processings such as encryption and decryption are speeded up by suppressing an increase of a load of a CPU in the processings.

SOLUTION: In a communication system wherein communication is performed using an encrypted transmission packet with an IP-SEC encryption system, the transmission packet is sent after **authentication** data in an **IP** -SEC **header** for decrypting IP-SEC encryption generated by the IP-SEC decryption of the transmission packet.

File 347:JAPIO Nov 1976-2003/Nov(Updated 040308)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200416
(c) 2004 THOMSON DERWENT

Set	Items	Description
S1	4032	TTL OR TIME(3W)LIVE
S2	66922	TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S3	145	IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5
S4	1186574	VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALID? OR CHECK?-?? ? OR CHEQU??? ? OR EXAMIN? OR TEST OR TESTS OR TESTED OR T-ESTING? OR EVALUAT? OR CONFIRM?
S5	22364	AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CRO-SSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQ?
S6	1653640	SCREEN? OR INSPECT? OR DETERMIN? OR ASSESS? OR MONITOR?
S7	198704	S4:S6(3N)(PACKET OR PACKETS OR CONTENT OR CONTENTS OR ECON-TENT? ? OR MESSAGE OR MESSAGES OR DATA OR FILE OR FILES OR OB-JECT OR OBJECTS)
S8	3	S1 AND S2:S3

8/9/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 THOMSON DERWENT. All rts. reserv.

015421844
WPI Acc No: 2003-483984/200346
XRPX Acc No: N03-384762
Data packet transmission method in mobile IP
Patent Assignee: WUHAN POST & TELECOM INST SCI MIN (WUHA-N)
Inventor: YU S; ZHANG R
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
CN 1411231	A	20030416	CN 2002139183	A	20021017	200346	B

Priority Applications (No Type Date): CN 2002139183 A 20021017
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
CN 1411231	A			H04L-012/56	

Abstract (Basic): CN 1411231 A
NOVELTY - This invention discloses a method for a data packet transmission in mobile IP in which this invention uses network addrss conversion to replace original **tunnel** systemto realize data packet transmission between non-local agent and hometown agentto spread the form of mobile agent discovering message. Hometown agent operates on network address conversion when receiving the said message; and non-localagent adds a network address conversion lift for safeguarding TCP/UDP/ICMP and modifies value of **TTL** to 255 the same time when operating on network addrss covers to guarantee the data packets will not lose in transmission, increasing data transmission efficiency.
DwgNo 0/0
Title Terms: DATA; PACKET; TRANSMISSION; METHOD; MOBILE; IP
Derwent Class: W01
International Patent Class (Main): H04L-012/56
International Patent Class (Additional): H04M-011/06; H04Q-007/20
File Segment: EPI
Manual Codes (EPI/S-X): W01-A03B; W01-A06G2; W01-B05; W01-C05B1; W01-C05B3

8/9/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 THOMSON DERWENT. All rts. reserv.

014794824 **Image available**
WPI Acc No: 2002-615530/200266
System for constructing virtual multicast network
Patent Assignee: ZOOINNET (ZOOI-N); EGC & C LTD (EGCC-N)

Inventor: PARK H J; KIM Y; PARK H
Number of Countries: 100 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2002023100	A	20020328	KR 200129308	A	20010528	200266	B
WO 200298063	A1	20021205	WO 2002KR1003	A	20020528	200306	

Priority Applications (No Type Date): KR 200129308 A 20010528
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2002023100	A		1	H04L-012/28	
WO 200298063	A1	E		H04L-012/28	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

Abstract (Basic): KR 2002023100 A

NOVELTY - A system for constructing a virtual multicast network is provided to comprise a multicast agent installed in a user PC as well as a virtual multicast router having a multicast router function on a network, and to comprise a multicast management server for managing information on each virtual multicast router, so as to use a multicast service under non-multicast environments.

DETAILED DESCRIPTION - A virtual multicast router(30) performs a dynamic **tunneling** for data transceiving between the virtual multicast router(30) and other virtual multicast router/multicast agent, by using an IP **tunneling** /UDP(User Datagram Protocol) **tunneling** , and manages multicast membership information of the other virtual multicast router and multicast agents. The virtual multicast router(30) transmits multicast data to a multicast agent and other virtual multicast router participating in a specific multicast group, and transmits multicast data between virtual multicast routers. The virtual multicast router(30) checks whether a multicast router exists in a self sub network. If so, the virtual multicast router(30) plays a role of multicast repeater only. A multicast agent(52) uses a dynamic **tunneling** for multicast data transceiving with the virtual multicast router(30), and uses a UDP **tunneling** for the dynamic **tunneling** , then retransmits the data of the virtual multicast router(30) to a multicast application program. The multicast agent(52) limits to **TTL** (**Time** to **Live**) 0 by using an IP multicast while re-transmitting the data, to perform a re-multicast for an operating computer only. A multicast management server(20) performs an IP caching for the multicast agent(52) that requests a retrieval and the retrieved virtual multicast router(30), and performs a caching for the multicast agent(52) or an IP address of the virtual multicast router(30), and a network address as well as the multicast agent(52), an IP address of the nearest virtual multicast router retrieved by the virtual multicast router(30), and the network address.

pp; 1 DwgNo 1/10

Title Terms: SYSTEM; CONSTRUCTION; VIRTUAL; NETWORK
Derwent Class: W01
International Patent Class (Main): H04L-012/28
File Segment: EPI
Manual Codes (EPI/S-X): W01-A06

```
File 256:SoftBase:Reviews,Companies&Prods. 82-2004/Feb
         (c)2004 Info.Sources Inc
File   2:INSPEC 1969-2004/Feb W5
         (c) 2004 Institution of Electrical Engineers
File   6:NTIS 1964-2004/Mar W1
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2004/Feb W5
         (c) 2004 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Mar W1
         (c) 2004 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2004/Feb
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/Mar W1
         (c) 2004 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2004/Feb W5
         (c)2004 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2004/Feb W4
         (c) 2004 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Feb
         (c) 2004 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2004/Mar 11
         (c) 2004 The Gale Group
File 144:Pascal 1973-2004/Feb W5
         (c) 2004 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2004/Feb 27
         (c) 2004 EBSCO Publishing
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File 266:FEDRIP 2004/Jan
         Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2004/Mar 09
         (c) 2004 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 603:Newspaper Abstracts 1984-1988
         (c)2001 ProQuest Info&Learning

Set     Items   Description
S1      11093   TTL OR TIME(3W)LIVE
S2     467139   TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S3       1910   IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5
S4   13455295   VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALID? OR CHECK?-
             ?? ? OR CHEQU??? ? OR EXAMIN? OR TEST OR TESTS OR TESTED OR T-
             ESTING? OR EVALUAT? OR CONFIRM?
S5      68540   AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CRO-
             SSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQ?
S6    9805179   SCREEN? OR INSPECT? OR DETERMIN? OR ASSESS? OR MONITOR?
S7     671608   S4:S6(3N)(PACKET OR PACKETS OR CONTENT OR CONTENTS OR ECON-
             TENT? ? OR MESSAGE OR MESSAGES OR DATA OR FILE OR FILES OR OB-
             JECT OR OBJECTS)
S8          35   S1 AND S2:S3
S9           1   S8 AND S7
S10         12   S8 AND S4:S6
S11         10   S8/2001:2004
S12         21   S8 NOT S9:S11
S13         14   RD (unique items)
S14          9   S13 NOT DIODE?
?
```

File 696:DIALOG Telecom. Newsletters 1995-2004/Mar 10
(c) 2004 The Dialog Corp.
File 15:ABI/Inform(R) 1971-2004/Mar 11
(c) 2004 ProQuest Info&Learning
File 98:General Sci Abs/Full-Text 1984-2004/Feb
(c) 2004 The HW Wilson Co.
File 484:Periodical Abs Plustext 1986-2004/Mar W1
(c) 2004 ProQuest
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2004/Mar 11
(c) 2004 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2004/Mar 11
(c) 2004 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 610:Business Wire 1999-2004/Mar 11
(c) 2004 Business Wire.
File 369:New Scientist 1994-2004/Feb W5
(c) 2004 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
(c) 1999 AAAS
File 20:Dialog Global Reporter 1997-2004/Mar 11
(c) 2004 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2004/Mar 11
(c) 2004 McGraw-Hill Co. Inc
File 634:San Jose Mercury Jun 1985-2004/Mar 10
(c) 2004 San Jose Mercury News
File 647:CMP Computer Fulltext 1988-2004/Feb W5
(c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Feb W5
(c) 2004 IDG Communications

Set	Items	Description
S1	24382	TTL OR TIME(3W)LIVE
S2	186485	TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S3	11849	IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5
S4	7769813	VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALID? OR CHECK?-?? ? OR CHEQU??? ? OR EXAMIN? OR TEST OR TESTS OR TESTED OR T-ESTING? OR EVALUAT? OR CONFIRM?
S5	150441	AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CRO-SSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQ?
S6	6506919	SCREEN? OR INSPECT? OR DETERMIN? OR ASSESS? OR MONITOR?
S7	321685	S4:S6(3N)(PACKET OR PACKETS OR CONTENT OR CONTENTS OR ECON-TENT? ? OR MESSAGE OR MESSAGES OR DATA OR FILE OR FILES OR OB-JECT OR OBJECTS)
S8	62	S1(S)S2:S3
S9	0	S8(S)S7
S10	7	S8(S)S4:S6
S11	0	S10/2001:2004
S12	5	RD S10 (unique items)
S13	8	S8/2001:2004
S14	51	S8 NOT (S13 OR WIND()TUNNEL?)
S15	36	S14 NOT (TRANSISTOR? OR DIODE? ? OR TUNNEL()BAT)

15/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02367353 117541446
Internet's information highway potential
De Maeyer, Dirk
Internet Research v7n4 PP: 287-300 1997
ISSN: 1066-2243 JRNL CODE: NTRS
WORD COUNT: 8297

...TEXT: each such island there is a multicast router, an mrouter. Mrouters are connected via unicast **tunnels** . Each **tunnel** in the MBone has a

metric and a threshold, so that mrouters can find the most suited delivery path and calculate whether packets are allowed to travel through a **tunnel** , that is that their **time** -to- **live** is long enough to pass the **tunnel** . A thorough explanation of the MBone can be found in Deering (1995), Eriksson (1994), and...

15/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02031558 54897338
IP + ATM = MPLS
Fryer, John
Telecommunications v34n5 PP: 109-112 May 2000
ISSN: 0040-2494 JRNL CODE: TIE
WORD COUNT: 2497

...TEXT: of service (TOS) bits prior to the Differentiated Services (DiffServ-) standards, and an 8-bit **time** -to- **live** (ELM) field, copied from the EP header used to discard packets in the event of...

... a combination of the two. In addition, labels may be stacked, which provides mechanisms for **tunneling** through networks, where the label switching occurs on the top label of the stack.

Although...

15/3,K/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00887591 95-36983
MBone: The multicast backbone
Eriksson, Hans
Communications of the ACM v37n8 PP: 54-60 Aug 1994
ISSN: 0001-0782 JRNL CODE: ACM
WORD COUNT: 5264

...TEXT: topology, rapid changes will be a problem.

The threshold is the minimum time-to-live (**TTL**) that a multicast datagram needs to be forwarded onto a given **tunnel** . When sent to the network by a client, each multicast packet is assigned a specific **TTL** . For each mrouted the packets pass, the **TTL** will be decremented by 1. If a packet's remaining **TTL** is lower than the threshold of the **tunnel** that DVMRP wants to send the packet onto, the packet is dropped. With that mechanism ... the scope of a multicast datagram is by using thresholds. If a datagram has a **TTL** greater than the threshold, it will be forwarded onto the **tunnel** . Thresholds range between 0 and 255. The threshold levels chosen on the **tunnel** tries reflect both a geographic partitioning (e.g., keeping a local conference local) and a...

15/3,K/6 (Item 1 from file: 613)
DIALOG(R)File 613:PR Newswire

00101612 19990504LNTU008 (USE FORMAT 7 FOR FULLTEXT)
SSH Communications Security Licenses SSH IKE Toolkit to Sun Microsystems
PR Newswire
Tuesday, May 4, 1999 05:33 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 387

TEXT:

...for Sun's customers to deploy
IPSec and will enhance Sun's existing Security offerings.

IPSEC /IKE (Internet Key Exchange) helps in negotiating the parameters of
encrypted communications, like the encryption algorithm to be used, the **time** -to- **live** for the encrypted information in addition to the encryption keys
between two parties before the...

15/3,K/33 (Item 12 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

05184982 (USE FORMAT 7 OR 9 FOR FULLTEXT)
SSH Communications Security Licenses SSH IKE Toolkit to Sun Microsystems
PR NEWSWIRE
May 04, 1999
JOURNAL CODE: WPRW LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 380

...in negotiating the parameters of encrypted communications, like the encryption algorithm to be used, the **time** -to- **live** for the encrypted information in addition to the encryption keys between two parties before the...
?

File   9:Business & Industry(R) Jul/1994-2004/Mar 10
         (c) 2004 Resp. DB Svcs.
File 16:Gale Group PROMT(R) 1990-2004/Mar 11
         (c) 2004 The Gale Group
File 47:Gale Group Magazine DB(TM) 1959-2004/Mar 11
         (c) 2004 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2004/Mar 05
         (c)2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2004/Mar 11
         (c) 2004 The Gale Group
File 570:Gale Group MARS(R) 1984-2004/Mar 11
         (c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Mar 11
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Mar 11
         (c) 2004 The Gale Group
File 649:Gale Group Newswire ASAP(TM) 2004/Mar 10
         (c) 2004 The Gale Group

Set	Items	Description
S1	37668	TTL OR TIME(3W)LIVE
S2	141845	TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S3	19928	IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5
S4	7515171	VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALID? OR CHECK?-?? ? OR CHEQU??? ? OR EXAMIN? OR TEST OR TESTS OR TESTED OR T-ESTING? OR EVALUAT? OR CONFIRM?
S5	191068	AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CRO-SSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQ?
S6	5392174	SCREEN? OR INSPECT? OR DETERMIN? OR ASSESS? OR MONITOR?
S7	472625	S4:S6(3N)(PACKET OR PACKETS OR CONTENT OR CONTENTS OR ECON-TENT? ? OR MESSAGE OR MESSAGES OR DATA OR FILE OR FILES OR OB-JECT OR OBJECTS)
S8	67	S1(S)S2:S3
S9	1	S8(S)S7
S10	11	S8(S)S4:S6
S11	1	S10/2001:2004
S12	10	S10 NOT S11
S13	4	RD (unique items)
S14	6	S8/2001:2004
S15	37	S8 NOT (S14 OR S10 OR WIND()TUNNEL? OR DIODE? ? OR TUNNEL(-)BAT)
S16	11	RD (unique items)

16/3,K/1 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

07087468 Supplier Number: 59735366 (USE FORMAT 7 FOR FULLTEXT)
IP + ATM = MPLS.(Technology Information)
Fryer, John
Telecommunications, v34, n2, p56
Feb, 2000
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 2456

... of service (TOS) bits prior to the Differentiated Services (DiffServ) standards, and an 8-bit **time** -to- **live** (**TTL**) field, copied from the IP header used to discard packets in the event of a...a combination of the two. In addition, labels may be stacked, which provides mechanisms for **tunneling** through networks, where the label switching occurs on the top label of the stack.
Although...

16/3,K/6 (Item 6 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06312875 Supplier Number: 54537464 (USE FORMAT 7 FOR FULLTEXT)
SSH Communications Security Licenses SSH IKE Toolkit to Sun Microsystems.
PR Newswire, p1783
May 4, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 358

IPSEC /IKE (Internet Key Exchange) helps in negotiating the parameters of encrypted communications, like the encryption algorithm to be used, the **time** -to- **live** for the encrypted information in addition to the encryption keys between two parties before the...

16/3,K/9 (Item 9 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

04733973 Supplier Number: 46968915 (USE FORMAT 7 FOR FULLTEXT)
NOVELL INC PREVIEWS KEY NETWORK SERVICES FOR INTRANET USERS
Computergram International, n3063, pN/A
Dec 13, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 252

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...cache. Pages will be stored and updated based on frequency of use, file size and **time** -to- **live** dates. Novell's security services provide administrators with a comprehensive, firewall class security framework. The ...

...virtual private network services that enable intranets to extend securely over the Internet via encrypted **tunnelling** . The services will work in conjunction with IntranetWare's wide area network routing options. The...

16/3,K/11 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01670091 SUPPLIER NUMBER: 15048995 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The Internet Multicasting Service: Ted Turner, watch out! (Carl Malamud brings long-distance fax services and on-demand radio shows to the Internet) (includes related articles on how to fax and on the MBONE Internet Multicast Backbone)
RELease 1.0, v94, n2, p10(6)
Feb 18, 1994
ISSN: 1047-935X LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 2988 LINE COUNT: 00239

... or resource-reservation capabilities.
The MBONE machines aren't all directly connected. They communicate by " **tunneling** " through standard (unicast) routers (they make their packets look normal to intervening routers and reconstitute them at the far end of a hop). Packets from streams that are **time** -sensitive, such as **live** audio, are assigned **time** -to- **live** (**TTL**) values, which cause the packets to self-destruct if they haven't arrived at their...
?

File 347:JAPIO Nov 1976-2003/Nov(Updated 040308)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200416
(c) 2004 THOMSON DERWENT
File 348:EUROPEAN PATENTS 1978-2004/Feb W05
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040304,UT=20040226
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	113	AU='ACHARYA A':AU='ACHARYA ARUP C O NEC USA INC'
S2	1	AU='BEIGI M S M'
S3	15	AU='JENNINGS R'
S4	4	AU='JENNINGS R B'
S5	1	AU='JENNINGS RAYMOND'
S6	18	AU='SAILER R':AU='SAILER REINER'
S7	11	AU='VERMA D'
S8	19	AU='VERMA D C'
S9	12	AU='VERMA DINESH':AU='VERMA DINESH CHANDRA'
S10	1	S1 AND S2:S9

10/9/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015387376 **Image available**
WPI Acc No: 2003-448321/200342
XRPX Acc No: N03-357627

Internet protocol routing method through virtual private network, involves identifying requested content from clients by reading labels of all packets in reverse proxy and switching packets to appropriate server in server form

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: **ACHARYA A** ; SHAIKH A A; TEWARI R; **VERMA D C**
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030065711	A1	20030403	US 2001968127	A	20011001	200342	B

Priority Applications (No Type Date): US 2001968127 A 20011001
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030065711	A1		24	G06F-015/16	

Abstract (Basic): US 20030065711 A1

NOVELTY - A hyper text transfer protocol (HTTP) request received from each client (113) is inspected in forward proxy (114). A TCP/HTTP connection (115) is set with appropriate server (122) by assigning multiprotocol label switching (MPLS) labels to the packets constituting the connection. In a reverse proxy (120), labels on packets are read, packets are switched to appropriate server in server form (126) and regulated content is identified.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for IP packet routing apparatus.

USE - For routing IP packets from client to server using common MPLS labels through VPN.

ADVANTAGE - Enables efficient routing of web requests and high performance web switching by mapping application layer information onto labels without terminating TCP connections.

DESCRIPTION OF DRAWING(S) - The figure shows the overall network architecture of web switching apparatus.

client (113)
forward proxy (114)
TCP/HTTP connection (115)
reverse proxy (120)
appropriate server (122)
server form (126)
pp; 24 DwgNo 1d/11

Title Terms: PROTOCOL; ROUTE; METHOD; THROUGH; VIRTUAL; PRIVATE; NETWORK; IDENTIFY; REQUEST; CONTENT; CLIENT; READ; LABEL; PACKET; REVERSE; SWITCH; PACKET; APPROPRIATE; SERVE; SERVE; FORM
Derwent Class: T01; W01
International Patent Class (Main): G06F-015/16
File Segment: EPI
Manual Codes (EPI/S-X): T01-N02A2; T01-N02A3B; W01-A06B7E; W01-A06E1; W01-A06F2C; W01-A06F3
?

```
File 696:DIALOG Telecom. Newsletters 1995-2004/Mar 13
         (c) 2004 The Dialog Corp.
File  15:ABI/Inform(R) 1971-2004/Mar 13
         (c) 2004 ProQuest Info&Learning
File  98:General Sci Abs/Full-Text 1984-2004/Feb
         (c) 2004 The HW Wilson Co.
File 484:Periodical Abs Plustext 1986-2004/Mar W1
         (c) 2004 ProQuest
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2004/Mar 15
         (c) 2004 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2004/Mar 13
         (c) 2004 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2004/Mar 15
         (c) 2004 Business Wire.
File 369:New Scientist 1994-2004/Mar W1
         (c) 2004 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File  20:Dialog Global Reporter 1997-2004/Mar 15
         (c) 2004 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2004/Mar 15
         (c) 2004 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2004/Mar 13
         (c) 2004 San Jose Mercury News
File 647:CMP  Computer Fulltext 1988-2004/Feb W5
         (c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Mar W1
         (c) 2004 IDG Communications

Set     Items   Description
S1      28461   TTL OR TTF OR TIME(1W)(LIVE OR LIFE)
S2       1492   (HOP OR HOPS)(2N)(LIMIT??? ? OR LIMITATION? OR COUNT??? ? -
             OR ALLOW?)
S3       3069   (IP OR INTERNET OR PROTOCOL OR ICMP OR DNS)(1W)(FIELD? ? OR
              HEADER? ?)
S4     186896   TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S5      12026   IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5 OR SOCKS(-
             )V5 OR LAYER()(TWO OR 2)()FORWARD??? ? OR L2F
S6      83002   VPN OR VPNS OR VIRTUAL()PRIVATE()(NET OR NETWORK? ?)
S7     503333   ENCAPSULAT? OR WRAP???? ? OR INSULAT?
S8      38642   (SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHE-
             R?)(2N)(CONNECT???? ? OR CONNECTIVIT? OR CHANNEL? ? OR PATH? ?
              OR PATHWAY? OR PASSAGE? ?)
S9     135254   (SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHE-
             R?)(2N)(COMMUNICAT???? ? OR ACCESS OR ACCESS?? ? OR ACCESSING)
S10    104129   PRIVATE(1W)(NET OR NETS OR NETWORK?)
S11   7596202   VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALIDAT? OR CHEC-
             K??? ? OR CHEQU? OR EXAMIN? OR TEST OR TESTS OR TESTED OR TES-
             TING? OR EVALUAT? OR CONFIRM?
S12    150599   AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CRO-
             SSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQU?
S13       489   S1:S3(S)S4:S10
S14       131   S13(S)S11:S12
S15       240   S1:S2(S)S4:S10
S16        47   S15(S)S11:S12
S17        26   S16/2001:2004
S18        21   S16 NOT S17
```

```
S19          19   RD (unique items)
S20       52480   S4:S10(15N)S11:S12
S21          62   S14(S)S20
S22          23   S21/2001:2004
S23          31   S21 NOT (S22 OR S16 OR TUNNEL()BAT OR LOGIC OR TRANSIST? OR
                  CIRCUIT?)
S24          22   RD (unique items)
```

? t19/3,k/1,6-7,15

19/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01833717 04-84708
Multiprotocol label switching
Petrosky, Mary
UNIX Review's Performance Computing v17n8 PP: 53-55 Jul 1999
ISSN: 1098-7150 JRNL CODE: URPC
WORD COUNT: 1730

...TEXT: that the outgoing packet includes a label. The job of that first MPLS node includes **examining** the IP header, classifying the packet, assigning it a label, **encapsulating** the packet in an MPLS header, and forwarding it to the next hop. At the...

... simple functions: it looks up the label in a table, swaps labels, may decrement a **time** to **live** (**TTL**) field, and forwards the packet.

Interestingly, each label has only local significance. That is, at...

19/3,K/6 (Item 3 from file: 813)
DIALOG(R)File 813:PR Newswire

0726631 NE014
WELLFLEET ANNOUNCES APPLETALK UPDATE-BASED ROUTING PROTOCOL SUPPORT FOR ENTERPRISE NETWORKS

DATE: July 25, 1994 10:33 EDT WORD COUNT: 974

...expansion.

For instance, an AURP router receives an IP-encapsulated packet with a DDP header **hop count** field containing a value of 7. Prior to sending the packet to its final destination, the AURP router **checks** the appropriate "distance" metric in its RTMP table and determines that the packet must travel another 10 hops to reach its final destination. The AURP router then resets the **hop count** field of the DDP header to a value of 5, allowing the packet to reach...

19/3,K/7 (Item 1 from file: 635)
DIALOG(R)File 635:Business Dateline(R)

0514871 94-69266
Wellfleet announces AppleTalk Update-based Routing Protocol support for enterprise networks
Schultz, Sheryl
PR Newswire (New York, NY, US) s1 p1
PUBL DATE: 940725
WORD COUNT: 946
DATELINE: Billerica, MA, US

TEXT:

...expansion.

For instance, an AURP router receives an IP-encapsulated packet with a DDP header **hop count** field containing a value of 7. Prior to sending the packet to its final destination, the AURP router **checks** the appropriate "distance" metric in its RTMP table and determines that the packet must travel another 10 hops to reach its final destination. The AURP router then resets the **hop count** field of the DDP header to a value of 5, allowing the packet to reach...

19/3,K/15 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01079942 CMP ACCESSION NUMBER: CWK19960129S0063
Why Wait for ATM? Frame-Relay Carries Voice Traffic Right Now
LOUIS CONNOR
COMMUNICATIONSWEEK, 1996, n 594, PG36
PUBLICATION DATE: 960129
JOURNAL CODE: CWK LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: WAN Services & Equipment
WORD COUNT: 1070

... want to wait for ATM to start saving money and who don't have huge **private networks** . At least one major carrier said, off the record, that its voice-over- frame-relay...

...summer debut. Indeed, Hypercom Inc. and ACT Networks are both reportedly in the process of **testing** frame-relay access devices (FRADs) designed to accomplish the **hop - limit** task.
Overall, frame-relay is most suitable for carrying voice in a corporate configuration where...
? t19/3,k/18-19

19/3,K/18 (Item 3 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

042312
Beware of frame relay gotchas
Feature
So you're ready to make the jump to frame relay? Well, you might want to consider the common pitfalls and how best to avoid them.
Byline: Christine Heckart
Journal: Network World Page Number: 36
Publication Date: February 06, 1995
Word Count: 3646 Line Count: 330

Text:
... when a link between two sites fails. Enabling split horizon makes perfect sense in a **private** -line **network** but not in a frame relay network. In a frame relay network, a single physical...interface to the router, while other mission-critical transactions could be hiding in TCP/IP- **encapsulated** telnet packets. Also, prioritization within the router is only one part of the answer. The...

... only routing protocols. Distance-vector protocols, such as the Routing

Information Protocol (RIP), use a **hop count** to determine the best available path. The path with the fewest number of intermediate hops... implements source route bridging (SRB), Data Link Switching (DLSw) or some other approach to SNA **tunneling** , or SDLC-to-LLC conversion. Frame Relay Assemblers/Disassemblers (FRAD) offer a similar solution. Many...broadband network services and other advanced telecommunications technologies. She can be reached via MCImail at **checkart** or 696-6902.

19/3,K/19 (Item 4 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

042283
Vendors plan wireless net connections
Byline: Joanie Wexler
Journal: Network World Page Number: 6
Publication Date: February 06, 1995
Word Count: 526 Line Count: 51

Text:
... because their applications have been designed for that carrier's net. The application portability also **allows** users to **hop** on another network if their net of choice does not have coverage in a given...

... backbone. The GTE net, though, would recognize the transmission as IP-based and automatically apply **IP security** to the **communication** , said Chuck Napier, director of distributed management-mobile data services at GTE PCS. ``This is...

... Laube, national director of information technology at Price Waterhouse in Menlo Park, Calif., which is **testing** CDPD. Napier said Motorola, Inc., Pacific Communication Sciences, Inc. and Sierra Wireless, Inc. are building ...

24/3,K/1 (Item 1 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00730076
NETWORK ADDRESS TRANSLATION IS NO SUBSTITUTE FOR IPV6 DEPLOYMENT
Communications Standards News
May 23, 2000 VOL: DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 2104 RECORD TYPE: FULLTEXT

TEXT:
...transparency of end-to-end connectivity
for transports that rely on the consistency of the **IP header** , and for protocols
that carry that address information in places other than the **IP header** . Using a
patchwork of consistently configured Application Layer Gateways (ALG's), endpoints can work around...stack modifications to enable the technology.

Firewalls are a Smaller Problem Because they Function as **Insulators**

Clearly, firewalls also break the End-to-End principle and raise several of the same...explosion of NATs is the impact on the deployment of network layer End-to-End **IP security** . A fundamental issue for **IP Security** is
that with both AH and ESP, the **authentication check** covers the TCP/UDP **checksum** ,
which in turn covers the IP address. When a NAT changes the IP address, the **checksum** calculation will fail, and **authentication** is guaranteed to fail.
Attempting to use the NAT as a security boundary fails when...

...subject to collisions when companies using these addresses merge
or want to directly interconnect using **VPNs** .
* NATs facilitate concatenating existing private name spaces with the public DNS.
* NAT versions like RSIP increase operational complexity when publicly published services reside on the private side.
* NATs invalidate the **authentication** mechanism of SNMPv3. Products may embed a NAT function without identifying it as such.
NATs...

24/3,K/2 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01834801 04-85792
IPsec
Allard, Johan; Nygren, Svante
Data Communications v28n9 PP: 63-76 Jun 1999
ISSN: 0363-6399 JRNL CODE: DCM
WORD COUNT: 2260

...TEXT: layers higher than IP, such as TCP or UDP and the packet's payload. In **tunnel** mode, the device **authenticates** and encrypts the

entire source packet and **wraps** a new **IP header** around it.

IPsec gateways work only in tunnel mode, which means no part of the original packet is...

24/3,K/3 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01763121 04-14112
Security on the new digital network
Loshin, Pete
Telecommunications (Americas Edition) v33n1 PP: 36-37 Jan 1999
ISSN: 0278-4831 JRNL CODE: TEC
WORD COUNT: 1542

...TEXT: on protocols that digitally sign the entire contents of IP packets for data integrity and **authentication** . For the most protection, organizations communicating over the Internet can use **IPsec** encryption on packets sent between security gateways-but this also means that the packets are...

24/3,K/4 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01723902 03-74892
Making the move to VPN tunnelling
Bitan, Sarah
Telecommunications (International Edition) v32n10 PP: 87-88 Oct 1998
ISSN: 0040-2494 JRNL CODE: TIE
WORD COUNT: 1583

ABSTRACT: The Internet protocol security (**IPSec**) standard is becoming the workhorse for interoperable network encryption. A series of guidelines for the protection of Internet protocol (IP) communications, **IPSec** specifies ways for securing private information transmitted over public networks. **IPSec** works in 2 ways. The first, **transport mode** , is the native way. The 2nd method is **tunnel** mode. Here, IP traffic generated by hosts without **IPSec** support is captured from the wire by a security device, or gateway. The gateway **encapsulates** the entire IP packet with **IPSec** encryption, including the original **IP header** . It then adds a new **IP header** to the data packet and sends it across the public network to a 2nd gateway, where the information is decrypted and sent in its original form to the designated recipient. **Tunnelling** is performed by a **VPN** device that resides at the entrance/exit points of a network. The device modifies outgoing traffic and decrypts and **authenticates** incoming data according to the methods outlined by **IPSec** . When using **tunneling** over the Internet, companies can build secure wide area networks, intranets and extranets at a...

24/3,K/5 (Item 4 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01694601 03-45591
RedCreek Communications offers users more VPN security options

Pappalardo, Denise
Network World v15n36 PP: 21 Sep 7, 1998
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 334

...TEXT: how they send traffic over the 'Net.

For example, Ravlin 3.0 adds support for **IPSec Encapsulating** Security Payload (ESP) transport to enable device-todevice encryption. The software also supports **authentication** header **tunneling** , which **encapsulates** only the header of an IP packet. In addition, the package adds **authentication** header transport support for device-todevice **IP header encapsulation** .

Prior to RedCreek's Ravlin 3.0 release, the software sup ported only IPSec ESP...

24/3,K/6 (Item 5 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01254063 99-03459
Authentication and privacy headers coming to your network's IP packets
Stallings, William
Network World v13n30 PP: 37 Jul 22, 1996
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 861

...TEXT: security features are implemented as extensions that follow the main IP header. The extension for **authentication** is known as the **Authentication** header and the one for privacy is called the **Encapsulating** Security Payload (ESP) header.

The **Authentication** header provides data integrity and allows for the **authentication** of IP packets. It includes an identifier of a particular security association between two parties...

24/3,K/7 (Item 6 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01223263 98-72658
IP next generation overview
Hinden, Robert M
Communications of the ACM v39n6 PP: 61-71 Jun 1996
ISSN: 0001-0782 JRNL CODE: ACM
WORD COUNT: 7498

...TEXT: Katz, Tony Li, Yakov Rekhter, Bill Simpson, and Sue Thompson.

Reference: References

1. Atkinson, R. **IP Security** Architecture. RFC,1825, August 1995. 2. Atkinson, R. **IP Authentication Header** . RFC-1826, August 1995. 3. Atkinson, R. IP **Encapsulating** Security Payload (ESP). RFC-1827, August 1995.

4. Bradner, B. and Mankin, A. The Recommendation...

24/3,K/9 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire

1164659 NEW002
OpenROUTE Networks Announces Expanded Capabilities For Its 'ALLWays.Secure' Network Security Portfolio

DATE: October 8, 1997 09:59 EDT WORD COUNT: 751

... Internet." Sun and OpenROUTE Networks have previously announced plans for joint sales and marketing activities.

VPNs connect sites within an organization's Intranet over a public network such as the Internet. The **VPN** provides data encryption and **authentication** to guarantee the privacy of the organization's information while it passes over the public network. **VPNs** use IP **Tunnels** to transport packets of data between the local router and remote locations. An IP **tunnel** **encapsulates** an IP packet which is addressed to a network within the remote site. The inner IP packet is usually encrypted and signed by the virtual interface before the outer **IP** **header** is applied. This forms an opaque, **authenticated** envelope that can securely transport the original packet from the local router to the remote location. The router or other **VPN** gateway at the other end then **checks** the packet signature to **verify** that the packet is not from an impostor. After it **checks** , the router then sends the data to the appropriate location, guaranteeing complete data privacy.

OpenROUTE...

24/3,K/10 (Item 1 from file: 613)
DIALOG(R)File 613:PR Newswire

00290393 20000313LAM009 (USE FORMAT 7 FOR FULLTEXT)
Netscreen Announces the Netscreen-1000 Gigabit Security System
PR Newswire
Monday, March 13, 2000 08:00 EST
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 678

...GigaScreen ASIC's encryption engine
delivers 1.2 Gbps DES encryption and 400 Mbps 3DES **IPSec** encryption with or
without simultaneous **authentication** . The **authentication** acceleration engine
supports both the MD5 and SHA-1 algorithms. In addition, its firewall engine
provides TCP/ **IP** **header** parsing, stateful inspection session lookup, network
address translation and a flexible policy search engine capable...

24/3,K/11 (Item 1 from file: 610)
DIALOG(R)File 610:Business Wire

00015970 1999073B1404 (USE FORMAT 7 FOR FULLTEXT)
RADLAN's OPAL ASIC-based Routing Engine RADLAN Announces OPAL ASIC-based One-armed Router for Layer 2 Switch Platforms
Business Wire
Sunday, March 14, 1999 13:42 EST
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 425

...filtering and provides detailed reporting on all Layer-3 traffic. In addition, the OPAL performs **IP header checksum validation** , re- **encapsulation** and handles local station forwarding as well as ICMP forwarding.

When integrating the OPAL with...

24/3,K/12 (Item 1 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

08856289
Netscreen unveils world's first gigabit Asic chip
Security vendor Netscreen has unveiled what it says is the world's first
NEWSWIRE (VNU)
December 23, 1999
JOURNAL CODE: WNEW LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 251

... merchant silicon now available.As a silicon based stateful inspection firewall, the Asic features TCP/ **IP header** parsing, Gigabit throughput network address translation (NAT) and a flexible policy search engine capable of...

24/3,K/13 (Item 2 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

01456048
Hi/Fn(TM) 7711 Encryption Processor(TM) Shipping -2-
PR NEWSWIRE
April 23, 1998 9:21
JOURNAL CODE: WPRW LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 288

...robbing packet fragmentation that often results from the additional overhead created by the IPSec security **protocol header** . The Hi/fn 7711 Encryption Processor specializes in performing the kinds of computations that slow...

24/3,K/14 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01225038 CMP ACCESSION NUMBER: NWC20001016S0032
VPN IPsec: Progress Slow But Steady - Despite the acceptance of the IPsec

standard, VPN management capabilities and interoperability are still lacking. Be sure of your exact needs before you buy.
Mike Fratto
NETWORK COMPUTING, 2000, n 1120, PG127
PUBLICATION DATE: 001016
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Feature
WORD COUNT: 2730

... SOHO situations where multiple computers are sharing a single Internet connection.

However, NAPT can break **IPsec VPNs** in two ways. If the **IPsec VPN** uses AH (**authentication** header), the **VPN** will fail because parts of the **IP header** , such as the IP addresses, have been digitally signed and can't be changed. NAPT also breaks **IPsec** in cases where the **VPN** is using ESP (**Encapsulated** Security Protocol) **tunnel** mode. ESP is simply an IP packet with no TCP/UDP information available. The NAPT...
...s ISB2LAN can help in this regard. The ISB2LAN can support up to 100 multiple **IPsec VPNs** through NAPT. It does this by tracking the IKE (Internet Key Exchange) negotiation between the **VPN** end points and mapping unique information from both ends to a translation table. The ISB2LAN then knows where to send packets when they are received. We **tested** this with multiple Cisco Secure **VPN** software clients connecting to our Cisco 7140. From the clients' point of view, the NAT didn't pose a problem. Nexland claims it can pass most vendors' **VPN** traffic without a problem.

Another option to pass IPsec VPN through a NAT or NAPT...

24/3,K/15 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01196477 CMP ACCESSION NUMBER: EET19990719S0058
IPv6 adds reliability features to Net
Joe Vallone, Technical Networking Specialist, Integrated Systems Inc., Dallas
ELECTRONIC ENGINEERING TIMES, 1999, n 1070, PG64
PUBLICATION DATE: 990719
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: COMMUNICATIONS - FOCUS: RELIABILITY ISSUES
WORD COUNT: 1350

... capability.

As for security, IPv6 builds two special schemes into the basic protocol to handle **authentication** and confidentiality: **IP Authentication Header** (AH) and IP **Encapsulating** Security Payload (ESP) . The AH is an extension header that provides integrity and **authentication** for IP packets. While many different **authentication** techniques are supported, use of the keyed Message Digest 5 (MD5) algorithm is required to ensure interoperability. Placing host **authentication** information at the Internet Layer in IPv6 provides considerably more protection to higher layer protocols...

24/3,K/16 (Item 3 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01193180 CMP ACCESSION NUMBER: DAC19990607S0021
IPsec - IPsec may be an open standard, but that's no guarantee that different vendors' gear will work together. To assess interoperability, we put an even dozen products through their paces (IPsec Interoperability)
Johan Allard and Svante Nygren
DATA COMMUNICATIONS, 1999, n 2809, PG63
PUBLICATION DATE: 990607
JOURNAL CODE: DAC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Special Report - IP Rules!
WORD COUNT: 2213

... layers higher than IP, such as TCP or UDP and the packet's payload. In **tunnel** mode, the device **authenticates** and encrypts the entire source packet and **wraps** a new **IP header** around it.

IPsec gateways work only in tunnel mode, which means no part of the original packet is...

24/3,K/17 (Item 4 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01190912 CMP ACCESSION NUMBER: LTH19990503S0040
The Wolf At The Door - Service Providers Keep Building More Secure VPNs, And Keep Getting Blown Away By Cost, Complexity And The Criminal Mind.
Tim Wilson
TELE.COM, 1999, n 409, PG42
PUBLICATION DATE: 990503
JOURNAL CODE: LTH LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Feature Articles
WORD COUNT: 2334

... more expensive dedicated lines or toll calling services.

A chief method of securing dial-up **VPN** services is the point-to-point **tunneling** protocol (**PPTP**), which encrypts traffic from the remote device and then **encapsulates** it in an **IP header** that can be sent across the Internet or other IP connections. **PPTP** creates a safe " **tunnel** " across the public network, making it difficult for hackers to tap into the traffic or read the encoded data. Many early dial-up **VPN** services **verified** users via remote **authentication** dial-in user service (RADIUS) servers, which store information about users' identities and **verify** that they are who they say they are before granting access to the corporate network...

24/3,K/18 (Item 5 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01045873 CMP ACCESSION NUMBER: NWC19950301S0049
Checksums In An Ethernet Packet With TCP/IP (Reviews)

NETWORK COMPUTING, 1995, n 603, P132
PUBLICATION DATE: 950301
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Columnists
WORD COUNT: 117

TEXT:
Unlike the 16-bit IP **checksum** that covers only the 20-byte **IP header** and none of its data, the 16-bit TCP **checksum** protects the data **encapsulated** in IP. Normally, the DLC **checksum** , in this case, Ethernet'

24/3,K/19 (Item 1 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

077497
Ask Dr. Intranet
Byline: Steve Blass
Journal: Network World Page Number: 41
Publication Date: September 06, 1999
Word Count: 243 Line Count: 22

Text:
We're using **Check** Point 's SecuRemote software to provide **virtual private network** connectivity to our remote users, but we're running into difficulties with some ISP connections...

... uses one of two methods to exchange keys and encrypt data: FWZ (with or without **encapsulation**) or Internet Key Exchange (IKE). SecuRemote uses User Datagram Protocol (UDP) Port 259 to negotiate encryption and **authentication** information with FWZ, and uses UDP Port 500 with IKE. Once the connection is complete...

... in one of three ways. With FWZ, it encrypts the packet data and leaves the **IP headers** alone without **encapsulation** , or it **encapsulates** the encrypted packets in IP 94 packets. With IKE, it **encapsulates** the encrypted packets in IP 50 packets. To solve your connectivity problems, you either have...

24/3,K/20 (Item 2 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

075475
Virtual private nets show QoS no respect
Byline: JIM DUFFY AND TIM GREENE
Journal: Network World Page Number: 1
Publication Date: June 21, 1999
Word Count: 819 Line Count: 76

Text:
Users looking for quality of service from their **VPNs** may be in for a rude awakening.It may be difficult for service providers to differentiate QoS on **virtual private networks** (**VPN**) built with encrypted **tunnels** because encryption scrambles the data in the IP packet vital for defining and requesting QoS...

...the key issues, and it is one of the arguments that says to me that **VPNs** as a service may not make sense," says John Freeman, an analyst at Current Analysis...

... look into the packet," says Dave Passmore, president of consultancy NetReference, also in Sterling. The **VPN** **tunneling** and encryption-standard IP Secur-ity (**IPSec**), for example, encrypts both the payload and header portions of an IP packet, Freeman says...

... Differentiated Services (Diff-Serv) - reside."Any ToS bits that have been set are scrambled" by **IPSec** , Freeman says.Likewise, if the **VPN** is set up using the common **tunneling** protocol called Layer 2 **Tunneling** Protocol (**L2TP**), the network being **tunneled** through may have trouble figuring out what QoS to grant to what applications. That is because the **L2TP** protocol does not address how to ensure QoS via Diff-Serv or the IETF's...

... bits within the encrypted header to an unencrypted, or "clear text" header ahead of the **tunneled** packet. Cisco has been shipping this capability in IOS 12.0 since January, says Richard...

... got it all integrated into one platform," says Karen Barton, vice president of marketing for **VPN** switch vendor Xedia in Littleton, Mass. "If you have two different pieces of equipment on either end of the **VPNs** . . . we couldn't make any representation about the ability to provide a QoS guarantee to...

... port number field of the IP packet, which is deeper within the packet than the **IP** **header** . If this information is left unencrypted, it's an invitation for hackers, analysts say."Now...

... It does compromise security."Right now, service providers are throwing bandwidth at the policy-based **VPN** QoS encryption problem. For example, Concentric Networks uses Xylan gear to queue traffic according to...

... capacity at it," which is inefficient, says John Lawler, Concentric's product line manager for **VPNs** . The IETF is currently working on ways for service providers to simplify their **VPN** QoS schemes.Some vendors and analysts say label switching schemes, such as the IETF's MPLS, solve the **VPN** QoS problem because they create closed user groups in which certain sites are only able...

...encryption is not needed, they say.Still, there will be some enterprises that insist on **tunneling** all **VPN** traffic. And things could become even more complicated when Microsoft releases Windows 2000, which is currently undergoing beta **testing** . Windows 2000 calls for using **L2TP** and **IPSec** , which Microsoft says are valuable for encrypting and **tunneling** non-IP packets across an IP **VPN** . But this "double **tunneling** " shields QoS information from MPLS routers, says Greg Marcotte, vice president of marketing for Altiga...
... make would be based on the source and destination IP addresses as shown in the **L2TP** packet header. Individual applications between two IP addresses could not be given different QoS levels, Marcotte says. The IETF is considering two proposals to overcome this. One describes how two **L2TP** devices could negotiate a Diff-Serv indicator for dial-in users. The other describes how...

24/3,K/21 (Item 3 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

068831
A recipe for a new flavor of VPN services
Byline: Denise Pappalardo
Journal: Network World Page Number: 33
Publication Date: September 14, 1998
Word Count: 567 Line Count: 55

Text:
Your ISP may be brewing a new class of **virtual private network** (**VPN**) services that will couple security, bandwidth management and guaranteed quality of service (QoS), but you...

... until early next year. Some ISPs will be turning to Xedia to bring the new **VPN** services to business users. Xedia's new Access Point QVPN gateways will let ISPs develop **VPN** services that give users the opportunity to define class-of-service measurements over their virtual...

... is expected to introduce its Access Point QVPN gateways next month. The devices will integrate **IP Security** (**IPSec**); Differentiated Services (Diff-Serv), a pending IETF QoS specification; and class-based queuing (CBQ) bandwidth...
... and large enterprise business users. One device can support up to 4,000 simultaneous encrypted **tunnels** , a source says. Corporate Technology Group, a Hunt Valley, Md., network integrator, wants to **check** out Access Point QVPN, says Eric Younkin, director of telecommunications.Corporate Technology Group is supporting...

... users securely, he says.For the first time, Xedia is supporting the IETF's pending **IPSec** protocol that defines encryption and **authentication** parameters for IP traffic. Xedia is using an "off the shelf" **IPSec** PCI card in Access Point QVPN, one source says. Xedia is also supporting X.509 digital certificates for user and network **authentication** . X.509 support will let service providers offer their customers the most secure user **authentication** available today. Xedia is using Verisign and Entrust certificate authorities to issue, distribute and maintain its ISP customers' digital certificates. While today business users and ISPs can deploy their own **IPSec VPN** equipment, they are limited when it comes to integrated QoS features, Renaissance's Morency says. Xedia's CBQ technology lets users carve out and dedicate chucks of their **VPN** bandwidth based on traffic type, IP address or URL.The company's Diff-Serv support lets users mark packets using the type of service (TOS) portion of an **IP header** . By using standard TOS code points, users will be able to send their traffic as...

24/3,K/22 (Item 4 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

068552
RedCreek offers users more VPN security options
Byline: Denise Pappalardo
Journal: Network World
Publication Date: August 28, 1998
Word Count: 322 Line Count: 31

Text:
RedCreek on Monday rolls out the latest version of software for its **VPN**

Ravlin hardware encryption devices.Ravlin 3.0 supports three more features that are part of the IETF's pending **IPSec** protocol. **IPSec** is a standards-based specification that defines **security** for private **communications** across an enterprise network. The new features will let users choose how they will send traffic over the public Internet. Ravlin 3.0 adds support for **IPSec** ESP transport, to enable device-to-device encryption. The software now supports **Authentication** Header (AH) **tunneling** which only **encapsulates** the header of an IP packet and AH transport for device-to-device **IP header encapsulation** . AH does not support any encryption, only **encapsulation** , which is not as secure.Until now, Ravlin only supported **IPSec** ESP **tunneling** , which lets users encrypt their data packets and **encapsulate** the packet's **IP header** , explains Cary Hayward, product marketing manager at RedCreek. ESP **tunneling** is the strongest, most secure way to transport packets over the public Internet, but it...

...says.For the first time Ravlin 3.0 will let users send traffic using AH **encapsulation** **tunneling** when they have less critical traffic to transport, while other users on the same **VPN** use ESP encryption **tunneling** because they are dealing with sensitive information. By using both methods users can sustain better...
?

```
File   9:Business & Industry(R) Jul/1994-2004/Mar 12
         (c) 2004 Resp. DB Svcs.
File  16:Gale Group PROMT(R) 1990-2004/Mar 15
         (c) 2004 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2004/Mar 15
         (c) 2004 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2004/Mar 09
         (c)2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2004/Mar 15
         (c) 2004 The Gale Group
File 570:Gale Group MARS(R) 1984-2004/Mar 15
         (c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Mar 15
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Mar 15
         (c) 2004 The Gale Group
File 649:Gale Group Newswire ASAP(TM) 2004/Mar 12
         (c) 2004 The Gale Group

Set     Items   Description
S1      42722   TTL OR TTF OR TIME(1W)(LIVE OR LIFE)
S2       1950   (HOP OR HOPS)(2N)(LIMIT??? ? OR LIMITATION? OR COUNT??? ? -
             OR ALLOW?)
S3       4217   (IP OR INTERNET OR PROTOCOL OR ICMP OR DNS)(1W)(FIELD? ? OR
              HEADER? ?)
S4     141890   TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S5      20262   IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5 OR SOCKS(-
            )V5 OR LAYER()(TWO OR 2)()FORWARD??? ? OR L2F
S6     133840   VPN OR VPNS OR VIRTUAL()PRIVATE()(NET OR NETWORK? ?)
S7     627017   ENCAPSULAT? OR WRAP???? ? OR INSULAT?
S8      55886   (SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHE-
            R?)(2N)(CONNECT???? ? OR CONNECTIVIT? OR CHANNEL? ? OR PATH? ?
             OR PATHWAY? OR PASSAGE? ?)
S9     185959   (SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHE-
            R?)(2N)(COMMUNICAT???? ? OR ACCESS OR ACCESS?? ? OR ACCESSING)
S10    183832   PRIVATE(1W)(NET OR NETS OR NETWORK?)
S11   7385438   VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALIDAT? OR CHEC-
            K??? ? OR CHEQU? OR EXAMIN? OR TEST OR TESTS OR TESTED OR TES-
            TING? OR EVALUAT? OR CONFIRM?
S12    191125   AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CRO-
            SSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQU?
S13       589   S1:S3(S)S4:S10
S14       123   S13(S)S11:S12
S15        97   S14 NOT (WIND()TUNNEL? OR TUNNEL()BAT OR DIODE? OR TRANSIS-
              TOR? OR LOGIC?)
S16        20   S15/2001:2004
S17        77   S15 NOT S16
S18        45   RD (unique items)

 18/3,K/1      (Item 1 from file: 9)
DIALOG(R)File   9:Business & Industry(R)
(c) 2004 Resp. DB Svcs. All rts. reserv.

2617830  Supplier Number: 02617830    (USE FORMAT 7 OR 9 FOR FULLTEXT)
TRAFFIC TUNERS -- Getting SNA's Benefits over the WAN -- Packeteer's
  Packetshaper manages bandwidth of legacy SNA traffic over IP networks
(Packeteer Inc's (Cupertino, CA) Packetshaper bandwidth management product
  is designed to boost branches' traditionally slow links)
Data Communications, p 19
```

October 21, 1999
DOCUMENT TYPE: Journal (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 692

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...agonizing process.

Legacy or IP?

Packetshaper sits behind the firewall on the local-area network, **examining** the contents of IP packets down to Layer 7 of the OSI stack (see the figure). It uses TCP windowing, meaning it looks at each packet and **checks** the acknowledgment control field in the TCP/ **IP header** . When it senses congestion, it modifies the acknowledgment control field and tells the server to...

...also follows preassigned policies and gives certain packets priority. For example, Packetshaper can recognize TN3270- **encapsulated** SNA packets and whisk them from corporate HQ to a branch office at the highest...

18/3,K/2 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

08073332 Supplier Number: 67336283 (USE FORMAT 7 FOR FULLTEXT)
Home connections need better security.(Technology Information)
Zarghami, Farshad
Electronic Engineering Times, p98
Nov 27, 2000
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2149

... in tunnel mode. Transport and tunnel modes are the two options for ESP implementations.

In **transport mode** , the original **IP header** is transmitted in the clear, meaning it is not compressed or encrypted. The ESP header, the upper-layer **protocol header** , and the payload follow the **IP header** . Then comes the ESP trailer, and if **authentication** is used, the ESP message- **authentication** code. In ESP **transport mode** , compression and encryption are performed on the TCP header and the payload. **Authentication** is performed over the ESP header, the TCP header, the payload and the ESP trailer...

...the security-based Soho router system design calls for authentication or encryption over the original **IP header** , there are two choices. The ESP **transport mode** is not one of them, since it is not defined to support this arrangement. Instead, the **authentication** header can be used in **transport mode** , although the **IPSec** subsystem would require two passes to perform the operation. The reason is that the compression operation must be performed before the total-length field in the **IP header** can be inserted and the total-length field must be used in the **authentication** . This would tax the subsystem more.

That alternative is tunnel-mode ESP, which processes the...

...a single pass in a security coprocessor, such as Hi/fn's 7951. In ESP

tunnel mode, the original header, TCP header and payload are compressed, encrypted, **authenticated** and **encapsulated** . A new **IP header** , which usually contains the source and destination addresses of gateways or firewalls, is inserted.

Authentication is performed over the ESP header, the original **IP header** (as with **authentication** header), the TCP header and the payload. Compression and encryption are performed on the original **IP header** , the TCP header and the payload. **Tunnel** -mode ESP provides **authentication** and encryption of the original **IP header** .

http://www.eetimes.com/

18/3,K/3 (Item 2 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

08030969 Supplier Number: 66101437 (USE FORMAT 7 FOR FULLTEXT)

VPN IPsec: Progress Slow But Steady -- Despite the acceptance of the IPsec standard, VPN management capabilities and interoperability are still lacking. Be sure of your exact needs before you buy.(Company Business and Marketing)

Fratto, Mike

Network Computing, p127

Oct 16, 2000

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 2913

... SOHO situations where multiple computers are sharing a single Internet connection.

However, NAPT can break **IPsec VPNs** in two ways. If the **IPsec VPN** uses AH (**authentication** header), the **VPN** will fail because parts of the **IP header** , such as the IP addresses, have been digitally signed and can't be changed. NAPT also breaks **IPsec** in cases where the **VPN** is using ESP (**Encapsulated** Security Protocol) **tunnel** mode. ESP is simply an IP packet with no TCP/UDP information available. The NAPT...

...s ISB2LAN can help in this regard. The ISB2LAN can support up to 100 multiple **IPsec VPNs** through NAPT. It does this by tracking the IKE (Internet Key Exchange) negotiation between the **VPN** end points and mapping unique information from both ends to a translation table. The ISB2LAN then knows where to send packets when they are received. We **tested** this with multiple Cisco Secure **VPN** software clients connecting to our Cisco 7140. From the clients' point of view, the NAT didn't pose a problem. Nexland claims it can pass most vendors' **VPN** traffic without a problem.

Another option to pass IPsec VPN through a NAT or NAPT...

18/3,K/4 (Item 3 from file: 16)

DIALOG(R)File 16:Gale Group PROMT(R)

07823634 Supplier Number: 65276679 (USE FORMAT 7 FOR FULLTEXT)

Do-It-Yourself: How to Set up a Windows 2000 Web Server.(Product Support)

Boyce, Jim

WinMag.com, pNA

Sept 15, 2000

Language: English Record Type: Fulltext Abstract

Document Type: Magazine/Journal; Trade

Word Count: 11072

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...SMTP (ESMTP).Outbound security: Specify security options for outbound connections to the remote domain, including **authentication** type, user account, and ...consideration is how you'll manage the server.(click image for expanded view)Create a **VPN** connection to a **VPN** server on the LAN where the Web server is located to enable remote administration through...

...have two primary options: use the Administration Web Site or use a dial-up or **VPN** connection. The Administration Web Site lets you manage existing Web sites and create new ones...
...through a RAS server and thereby become a member of the LAN or use a **VPN** connection to a **VPN** server on the LAN. Once connected in that way you can use the IIS console...

...limit, outgoing connection limit, timeout, and TCP port.The Access page controls several options, including **authentication** methods, certificates and SSL, connection control by IP address or subnet, and global relay restrictions...

...of options controlling message delivery. These include retry intervals, delay notification, expiration timeout, and outbound **authentication** options. You can also set advanced settings such as maximum **hop count** , smart host, and so on.(click image for expanded view)You can limit session size...

18/3,K/5 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

07504973 Supplier Number: 62350504 (USE FORMAT 7 FOR FULLTEXT)
E-Business Security.(NetScreen-1000 data security system from NetScreen Technologies)(Product Announcement)
Telecommunications, v34, n4, p81
April, 2000
Language: English Record Type: Fulltext
Article Type: Product Announcement
Document Type: Magazine/Journal; Trade
Word Count: 270

... s ASIC's encryption engine delivers 1.2-Gbps DES encryption and 400-Mbps 2DES **IPSec** encryption with or without simultaneous **authentication** . The **authentication** acceleration engine supports both the MD5 and SHA-1 algorithms, and its firewall provides TCP/ **IP headers** parsing, stateful inspection lookup, network address translation, and a policy search engine capable of searching...

18/3,K/6 (Item 5 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

07098807 Supplier Number: 60002607 (USE FORMAT 7 FOR FULLTEXT)
Ixia Demonstrates Three Exciting New Products -- Its OC-48c Packet Over SONET Interface, Its QoS Performance Tester and Its Terabit Router Tester.
Business Wire, p0327
March 6, 2000

Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 722

... 48c Packet Over SONET Interface. The IXIA LMOC48c Load Module is a comprehensive tool for **verifying** terabit routers with WAN Packet Over SONET/SDH interfaces operating at the OC-48 level...

...1619/1662, with the addition of 1+X43 payload scrambling, as well as Ciscos HDLC **encapsulation** of IP packets. As with all Ixia Load Modules, the LMOC48c offers users extreme configuration flexibility, including **IP header** contents (incrementing, decrementing, or random IP addresses), fixed or algorithmic data patterns, insertable 32-bit...

18/3,K/7 (Item 6 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

07082916 Supplier Number: 59700918 (USE FORMAT 7 FOR FULLTEXT)
Your Own Private Internet - The Internet didn't invent the idea of sharing data between organizations-it just perfected it. Here's how to create the perfect extranet for your organization.(Company Business and Marketing)
Linthicum, David
Computer Shopper, p236
April, 2000
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1858

... which, as we mentioned, typically costs more to implement and maintain.

In the world of **VPNs** , **IPSEC** is the security standard of choice for most vendors, and you should look for it when you select **VPN** products. **IPSEC** is a group of protocols described by the Internet Engineering Task Force (IETF). Mandatory to this specification is the notion of protocol **authentication** , privacy, and data integrity at the IP or kernel level. **IPSEC** uses two optional **IP headers** : **Authentication** Header (AH), which supports **authentication** and data integrity, and **Encapsulating** Security Payload (ESP), for privacy. **IPSEC** presents design goals for a top- level, component-oriented structure rather than detailing specific encryption...

18/3,K/8 (Item 7 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06756727 Supplier Number: 56894961 (USE FORMAT 7 FOR FULLTEXT)
TRAFFIC TUNERS -- Getting SNA's Benefits over the WAN -- Packeteer's Packetshaper manages bandwidth of legacy SNA traffic over IP networks.(Hardware Review)(Evaluation)
Bruno, Lee
Data Communications, p19
Oct 21, 1999
Language: English Record Type: Fulltext Abstract
Article Type: Evaluation
Document Type: Magazine/Journal; Trade
Word Count: 703

... agonizing process.
Legacy or IP?
Packetshaper sits behind the firewall on the local-area network, **examining** the contents of IP packets down to Layer 7 of the OSI stack (see the figure). It uses TCP windowing, meaning it looks at each packet and **checks** the acknowledgment control field in the TCP/ **IP** **header** . When it senses congestion, it modifies the acknowledgment control field and tells the server to...
...also follows preassigned policies and gives certain packets priority. For example, Packetshaper can recognize TN3270- **encapsulated** SNA packets and whisk them from corporate HQ to a branch office at the highest...

18/3,K/9 (Item 8 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06703121 Supplier Number: 56059647 (USE FORMAT 7 FOR FULLTEXT)
Toshiba Participates in Telecom 99 in Geneva.
PR Newswire, p2038
Oct 7, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 792

... with a self-healing function.
Multi Protocol Label Switching (MPLS)
A key technology for Dynamic **VPN** , MPLS achieves extremely high packet transfer speeds. Every packet in the network is assigned a...

...route separately from transfer processing. The label eliminates the extra load created by having to **examine** the **IP** **header** .
Infrastructure Access
Broadband Wireless Access System
As a "last mile" solution, broadband wireless access systems...

18/3,K/10 (Item 9 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06496620 Supplier Number: 55192939 (USE FORMAT 7 FOR FULLTEXT)
IPv6 adds reliability features to Net.(Internet/Web/Online Service Information)
Vallone, Joe
Electronic Engineering Times, p64
July 19, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1348

... capability.
As for security, IPv6 builds two special schemes into the basic protocol to handle **authentication** and confidentiality: **IP** **Authentication** **Header** (AH) and IP **Encapsulating** Security Payload (ESP). The AH is an extension header that provides integrity and **authentication** for IP packets. While many different **authentication** techniques are supported, use of the keyed Message Digest 5 (MD5) algorithm is required to ensure interoperability. Placing host **authentication** information at the Internet Layer in IPv6 provides considerably more

protection to higher layer protocols...

18/3,K/11 (Item 10 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06466345 Supplier Number: 54851730 (USE FORMAT 7 FOR FULLTEXT)
MULTIPROTOCOL LABEL SWITCHING. (new standard) (Internet/Web/Online Service Information) (Tutorial)
Petrosky, Mary
UNIX Review's Performance Computing, v17, n8, p53
July, 1999
Language: English Record Type: Fulltext Abstract
Article Type: Tutorial
Document Type: Magazine/Journal; Trade
Word Count: 1754

... that the outgoing packet includes a label. The job of that first MPLS node includes **examining** the **IP header** , classifying the packet, assigning it a label, **encapsulating** the packet in an MPLS header, and forwarding it to the next hop. At the...

...simple functions: it looks up the label in a table, swaps labels, may decrement a **time** to **live** (**TTL**) field, and forwards the packet.
Interestingly, each label has only local significance. That is, at...

18/3,K/12 (Item 11 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06393263 Supplier Number: 54812959 (USE FORMAT 7 FOR FULLTEXT)
IPsec -- IPsec may be an open standard, but that's no guarantee that different vendors' gear will work together. To assess interoperability, we put an even dozen products through their paces. (IPsec Interoperability) (Internet/Web/Online Service Information)
Allard, Johan; Nygren, Svante
Data Communications, p63
June 7, 1999
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 2208

... possible modes: In transport mode, IPsec devices reuse the original IP header. As a result, **IPsec** protection applies only to layers higher than IP, such as TCP or UDP and the packet's payload. In **tunnel** mode, the device **authenticates** and encrypts the entire source packet and **wraps** a new **IP header** around it.
IPsec gateways work only in tunnel mode, which means no part of the ...

18/3,K/13 (Item 12 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06385976 Supplier Number: 54789671 (USE FORMAT 7 FOR FULLTEXT)
Overhauled aeronautic net secured by IPSec. (Company Operations)
Network World, p37

May 31, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 476

... an opportunity to institute security policies based on the idea of segregating traffic types.
"The **VPNs** give you a type of service field in the **IP header** to allow routing equipment to distinguish different types of traffic," McShea says. That would make...

...possible to set boundaries on the use of sensitive data. The next step will be **testing** a large amount of network equipment in a lab environment to see what works best...

18/3,K/14 (Item 13 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06282297 Supplier Number: 54426645 (USE FORMAT 7 FOR FULLTEXT)
IBM Outlines Policy Management Architecture.
Computergram International, pNA
April 20, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 721

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...as 25 times faster than its rivals. Other enhancements to the CPE policy engine include **virtual private network** "enforcement" functions that will offer customers the choice of using Differentiated Service (DiffServ) or Integrated...

...QoS classes, which allow users to prioritize different traffic types, using 6 bits of the **IP header** as identity tags. Most DiffServ protocols are still under discussion in the IETF, and IBM...

...race to establish IP QoS credentials, are the immediate provision of two management tools. Policy **test** , an IP network simulator, will allow network managers to run theoretical traffic patterns against different...

...spot ptoentially disastrous conflicts (such as those associated with RSVP) before policies are executed live. **VPN tunneling** , on the other hand, provides a key link between the LDAP network device management environment, and the wider systems management capabilities of Tivoli. Using **VPN tunneling** , said Blenkhorn, customers will be able to identify traffic flows in terms of their security...

18/3,K/15 (Item 14 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06246497 Supplier Number: 54841436 (USE FORMAT 7 FOR FULLTEXT)
Public Key Infrastructure Basics.(Technology Information)
Farrow, Rik
Network, pNA
Jan 1, 1999

Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 1889

... YOUR OWN PKI
If an organization had its own PKI, it could use certificates for **IPSec** , a component of IPv6 that is supported by most **VPN** products. **IPSec** enables the **authentication** of **IP headers** with digital signatures (no spoofed source addresses), and provides encryption at layer 3. Layer-3...

...the network will use encryption with participating systems transparently-no modifications will be necessary. Current **IPSec** products require manual key exchange/configuration, but a functional PKI should solve this problem.
While...

18/3,K/16 (Item 15 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06190852 Supplier Number: 54095829 (USE FORMAT 7 FOR FULLTEXT)
RADLAN's OPAL ASIC-based Routing Engine RADLAN Announces OPAL ASIC-based One-armed Router for Layer 2 Switch Platforms.
Business Wire, p1404
March 15, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 393

... filtering and provides detailed reporting on all Layer-3 traffic. In addition, the OPAL performs **IP header checksum validation** , re-**encapsulation** and handles local station forwarding as well as ICMP forwarding.
When integrating the OPAL with...

18/3,K/17 (Item 16 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06101332 Supplier Number: 53667858 (USE FORMAT 7 FOR FULLTEXT)
Security on the New Digital Network.(Technology Information)
Loshin, Pete
Telecommunications, v33, n1, p36(1)
Jan, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1671

... data is encrypted as is transport and application protocol header information. The IP Security Architecture (**IPsec**) relies on protocols that encrypt the entire contents of IP packets for data security and...

...on protocols that digitally sign the entire contents of IP packets for data integrity and **authentication** . For the most protection, organizations communicating over the Internet can use **IPsec** encryption on packets sent between security gateways--but this also means that the packets are...

18/3,K/18 (Item 17 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06058765 Supplier Number: 54841573 (USE FORMAT 7 FOR FULLTEXT)
LAN-to-LAN VPNs: Secure Enough?(virtual private network)(Technology Information)
Steinke, Steve
Network, pNA
August 1, 1998
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 4249

... you can find the key IPSec RFCs: RFC1825 (Security Architecture for the Internet Protocol), RFC1826 (**IP Authentication Header**), and RFC1827 (IP **Encapsulating** Security Payload [ESP]). They can also be found at any other RFC repository.
ftp.isi...

18/3,K/19 (Item 18 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

05539643 Supplier Number: 48397447 (USE FORMAT 7 FOR FULLTEXT)
IPSec For Communities Of Interest
Moskowitz, Robert
Network Computing, p102
April 1, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2083

... you are doing. ESP also can use null encryption, which amounts to AH without the **authentication** of the **IP header** . This can allow for NAT traversal, since the addresses in the **IP header** are mutable.
ESP and AH are registered by the IANA (Internet Address Naming Authority) as...

18/3,K/20 (Item 19 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

05245258 Supplier Number: 47995704 (USE FORMAT 7 FOR FULLTEXT)
Unhook your leased lines
InfoWorld, p80
Sept 22, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 3085

... schemes, but the company's proprietary solution limits interoperability between non-FireWall-1 firewalls.
Manual **IPSec** , an earlier implementation of the **IPSec** standard, offers encryption, **authentication** , and **Check** Point's answer to the proposed Internet Security Association and Key Management Protocol (ISAKMP)/Oakley key-exchange draft. Because this solution is a firewall

implementation, it offers **IPSec** only in **tunnel** mode. In this scheme, the entire original packet (including the header) is encrypted and then an **encapsulating** security payload (ESP) header and a new **IP header** are attached.

We liked Check Point's implementation of this early IPSec draft because it...

18/3,K/21 (Item 20 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05198307 Supplier Number: 47931362 (USE FORMAT 7 FOR FULLTEXT)
Securing Internet VPNs
Kosiur, Dave
PC Week, p089
August 25, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 913

... data.

In the IPSec architecture, two datagram headers have been designed for different tasks. The **IP Authentication Header** , or AH, takes care of **authentication** and data integrity--assuring the receiver that a received datagram was in fact transmitted by...

...identified as the source and that the datagram wasn't altered since transmission. The ESP (**Encapsulating** Security Payload) header maintains the privacy of the IP datagrams by encrypting the contents.

To...

18/3,K/22 (Item 21 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04175235 Supplier Number: 46099115 (USE FORMAT 7 FOR FULLTEXT)
Why Wait for ATM? Frame-Relay Carries Voice Traffic Right Now
CommunicationsWeek, p36
Jan 29, 1996
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 1069

... want to wait for ATM to start saving money and who don't have huge **private networks** . At least one major carrier said, off the record, that its voice-over-frame-relay...

...summer debut. Indeed, Hypercom Inc. and ACT Networks are both reportedly in the process of **testing** frame-relay access devices (FRADs) designed to accomplish the **hop - limit** task.

Overall, frame-relay is most suitable for carrying voice in a corporate configuration where...

18/3,K/23 (Item 22 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

02948111 Supplier Number: 43988574 (USE FORMAT 7 FOR FULLTEXT)
The Point-to-Point Protocol: REMOTE USERS CAN FIND AN OASIS IN PPP
CommunicationsWeek, p544
July 26, 1993
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 2320

... should be used to interpret the data found in the Information field.

For instance, the **protocol field** may indicate that the information field contains an IP, IPX or AppleTalk packet, or a packet specific to a PPP-protocol, such as LCP or Password **Authentication** Protocol (PAP). The Information field is variable in length, growing up to a negotiated Maximum Receive Unit (MRU) size. All PPP packets contain a **checksum** stored in the Frame **Check** Sequence (FCS) field. The FCS field is calculated over the entire packet (excluding the delimiter...

...faults, such as noisy phone lines. By default only 8 additional bytes are required for **encapsulation** , and, with typical header compression negotiated, this is reduced to 4 bytes.

The establishment of...

18/3,K/24 (Item 1 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2004 The Gale group. All rts. reserv.

04565473 SUPPLIER NUMBER: 18593691
Securing private WANs on the Net. (authentication and encryption standards for the Internet)(PC Week Netweek) (Internet/Web/Online Service Information)
Kosiur, Dave
PC Week, v13, n33, pN1(2)
August 19, 1996
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1133 LINE COUNT: 00097

...ABSTRACT: equipment from different vendors. The IETF's IP Security Working Group (IPSec) has created the **IP Authentication Header** (AH) for data integrity and **authentication** . AH **verifies** the source of a message and guarantees that the message was not altered. The **Encapsulating** Security Payload (ESP) header provides the encryption that prevents the message from being seen by...
... Protecting the datagrams

IPSec has designed two different datagram headers for two different tasks. The **IP Authentication Header** , or AH, is supposed to take care of **authentication** and data integrity; that is, assuring the receiver that a received datagram was, in fact...

...identified as the source and that the datagram wasn't altered since transmission. The ESP (**Encapsulating** Security Payload) header is assigned a different role: that of maintaining the privacy of the...

18/3,K/25 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

12500662 SUPPLIER NUMBER: 63609378 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Remote Access VPNs: Selection And Deployment Issues. (Technology Information)
King, Christopher M.
Business Communications Review, 30, 6, 52
June, 2000
ISSN: 0162-3885 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2889 LINE COUNT: 00235

... PPTP and IPSec communications are disrupted. This is because the IP header fails the cryptographic **checksum** at the **VPN** gateway termination end. The RA- **VPN** client that connects to a **VPN** gateway must use a clear, publicly-routable IP address.
This is a problem, because many...

18/3,K/26 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

10346867 SUPPLIER NUMBER: 20956976 (USE FORMAT 7 OR 9 FOR FULL TEXT)
VPN standards tackle network apps. (the Automotive Industry Action Group's Automotive Network Exchange pilot project to build the world's largest virtual private network extranet) (Internet/Web/Online Service Information)
Carlson, David F.
Electronic Engineering Times, n1018, p86(1)
July 27, 1998
ISSN: 0192-1541 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1175 LINE COUNT: 00100

... authentication, privacy and data integrity at the IP or kernel level. It utilizes two optional **IP headers** : **Authentication** Header, which supports **authentication** and data integrity, and **Encapsulating** Security Payload, which ensures privacy.
'Tunneling' function
The term "tunneling" in the L2TP standard refers...

18/3,K/28 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

09906665 SUPPLIER NUMBER: 20052756
Bulletproof IP. (authentication and encryption for TCP/IP) (Internet/Web/Online Service Information)
Thayer, Rodney
Data Communications, v26, n16, p54(6)
Nov 21, 1997
ISSN: 0363-6399 LANGUAGE: English RECORD TYPE: Abstract

...ABSTRACT: all IP communications. IPSec protocols, which are still undergoing revision, fit in new fields in **IP** packet **headers** . **IPSec** protocols **validate** packets with a secret key shared by the sender and receiver, but do not encrypt its contents. That task is performed by **IPSec** codes. The combination of encryption and security promises strong TCP/ **IP security** . The ISPSec **authentication** header and **encapsulating** security payload define **authentication** and encryption methods for IP payloads, while the **IP security** association key management protocol manages the exchange of secret keys by senders and recipients.

18/3,K/29 (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

09773569 SUPPLIER NUMBER: 19833518 (USE FORMAT 7 OR 9 FOR FULL TEXT)
OpenROUTE Networks Announces Expanded Capabilities For Its 'ALLWays.Secure' Network Security Portfolio
PR Newswire, p1008NEW002
Oct 8, 1997
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 809 LINE COUNT: 00074

... inner IP packet is usually encrypted and signed by the virtual interface before the outer **IP header** is applied. This forms an opaque, **authenticated** envelope that can securely transport the original packet from the local router to the remote location. The router or other **VPN** gateway at the other end then **checks** the packet signature to **verify** that the packet is not from an impostor. After it **checks** , the router then sends the data to the appropriate location, guaranteeing complete data privacy.
OpenROUTE...

18/3,K/30 (Item 6 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

09648140 SUPPLIER NUMBER: 18422715 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Emerging standards back virtual secure tunnels.
Barbetta, Frank
Business Communications Review, v26, n5, p30(2)
May, 1996
ISSN: 0162-3885 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1350 LINE COUNT: 00113

... algorithms.
The RFCs define an "IPsec Security Association" and the elements common to both an **IP Authentication Header** (AH) and an IP Enapsulating Security Payload (ESP). "Security Associations" are not necessarily the same...

18/3,K/31 (Item 7 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

09647534 SUPPLIER NUMBER: 18307770 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Next-generation IP takes shape. (Internet Protocol)
Mendes, Gerald H.
Business Communications Review, v26, n3, p49(5)
March, 1996
ISSN: 0162-3885 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3339 LINE COUNT: 00267

... managed by a scheme called Internet Key Management Protocol (IKMP) that was created by the **IP Security** working group.
Another field in the Authentication header extension, called Security Index, is used by...

18/3,K/32 (Item 8 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

08843290 SUPPLIER NUMBER: 18537363
Authentication and privacy headers coming to your network's IP packets. (proposed Internet Engineering Task Force standards) (Technology Information)
Stallings, William
Network World, v13, n30, p37(1)
July 22, 1996
ISSN: 0887-7661 LANGUAGE: English RECORD TYPE: Abstract

...ABSTRACT: standards are RFC 1825 through RFC 1829. IP-level security involves two areas, which are **authentication** and privacy. Security arrangements are mandated for the next generation of IP, called IPv6, and is optional for the existing version, IPv4. For both **authentication** and privacy, the new security capabilities are implemented as extensions to the main IP header. The extension for **authentication** is called the **Authentication** header, and the extension for privacy is called the **Encapsulating** Security Payload (ESP) header. The **authentication** and privacy mechanisms can be combined.

18/3,K/33 (Item 9 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

08430146 SUPPLIER NUMBER: 17903137 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Why wait for ATM? Frame-relay carries voice traffic right now. (pros, cons of both standards) (Technology Information)
Connor, Louis
CommunicationsWeek, n594, p36(2)
Jan 29, 1996
ISSN: 0746-8121 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1139 LINE COUNT: 00089

... reportedly in the process of testing frame-relay access devices (FRADs) designed to accomplish the **hop - limit** task.
Overall, frame-relay is most suitable for carrying voice in a corporate configuration where...

18/3,K/34 (Item 10 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

07498576 SUPPLIER NUMBER: 15687748 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Is open architecture and Type-1 encryption an oxymoron?
Franklin, Robert W.
Defense Electronics, v26, n8, p21(3)
August, 1994
ISSN: 0278-3479 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2508 LINE COUNT: 00190

... header information) and the "safe" packet is sent to the black side where a new **IP header** is added.
This Transparent package allows us to process frames from over 150 separate protocols...

18/3,K/35 (Item 11 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

07475042 SUPPLIER NUMBER: 15609224 (USE FORMAT 7 OR 9 FOR FULL TEXT)
WELLFLEET ANNOUNCES APPLETALK UPDATE-BASED ROUTING PROTOCOL SUPPORT FOR ENTERPRISE NETWORKS
PR Newswire, p0725NE014
July 25, 1994
LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 1066 LINE COUNT: 00096

... value of 7. Prior to sending the packet to its final destination, the AURP router **checks** the appropriate "distance" metric in its RTMP table and determines that the packet must travel another 10 hops to reach its final destination. The AURP router then resets the **hop count** field of the DDP header to a value of 5, allowing the packet to reach...

18/3,K/39 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02408082 SUPPLIER NUMBER: 62652936 (USE FORMAT 7 OR 9 FOR FULL TEXT)
BROADBAND REPORT - What's on Broadband: 'Quantum Project'.(News Briefs)
Finnie, Scot
WinMag.com, NA
May 4, 2000
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1649 LINE COUNT: 00128

... what your IP address actually is at any given time can be important for both **connectivity** and **security** reasons.Windows 9x users have a convenient way of **checking** their IP address (as well as several other pertinent facts about their current Internet connection...

...in your Windows Folder in case you'd like to make a shortcut to it.) **Check** the " **IP** Address" **field** for your current IP address. If you have more than one adapter on your PC...

...list. It's often a good idea to click the Release and Renew buttons to **verify** your existing connection. And click the "More Info" button.IP Configuration is also a useful...
? t18/3,k/41-45

18/3,K/41 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02092473 SUPPLIER NUMBER: 19535406 (USE FORMAT 7 OR 9 FOR FULL TEXT)
IP for the next generation.(Internet Protocol) (Internet/Web/Online Service Information)
Held, Gilbert
Network, v12, n7, p65(6)
July, 1997
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4419 LINE COUNT: 00354

... not contain any optional elements, it allows separate extension headers to be placed between the **IP header** and the Transport-layer header. For example, **authentication** and security **encapsulation** is performed via extension headers and identified via the 8-bit Next Header field, which...

18/3,K/42 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02070868 SUPPLIER NUMBER: 19321573 (USE FORMAT 7 OR 9 FOR FULL TEXT)
IPv6: the next generation Internet Protocol. (Internet/Web/Online Service Information)
Kessler, Gary
Network VAR, v5, n2, p32(7)
Feb, 1997
ISSN: 1082-8818 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3855 LINE COUNT: 00340

... s). The only destination options defined so far are Pad1 and PadN, as described.

The **IP Authentication Header** (AH) and IP **Encapsulating** Security Payload (ESP) are IPv6 security mechanisms (see the section called IPv6 Security later in...security schemes; however, IPv6 builds two such security schemes into the basic protocol.

The IP **Authentication** Header is an extension header that provides integrity, **authentication** , and nonrepudiation for IP datagrams. The IP **Encapsulating** Security Payload is an extension header that provides integrity and confidentiality for IP datagrams. These...

18/3,K/43 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01707864 SUPPLIER NUMBER: 16306262 (USE FORMAT 7 OR 9 FOR FULL TEXT)
OSPF: addressing RIP's shortcomings. (the Open Shortest Path First routing protocol improves upon the Routing Information Protocol)
Molloy, Maureen
INTERNETWORK, v5, n9, p60(1)
Sept, 1994
LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 574 LINE COUNT: 00053

... level of urgency, as well as enabling traffic to be split amongst multiple least-cost **paths** .

For added **security** -- particularly when data is being sent over the public switched telephone network, an OSPF packet is also equipped with an **authentication** field in its header. This prevents routing information inside an OSPF router from being corrupted...

18/3,K/44 (Item 6 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01669454 SUPPLIER NUMBER: 15037333 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Remote access with SLIP and PPP. (the Serial Line Interface Protocol and Point-to-Point Protocol for transmitting TCP/IP over serial lines) (Net

Worth) (Column)
Baker, Steven
UNIX Review, v12, n3, p21(5)
March, 1994
DOCUMENT TYPE: Column ISSN: 0742-3136 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2522 LINE COUNT: 00200

... bit protocol field that allows PPP to multiplex traffic for several network layers (NCPs). This **encapsulation** frame has a 16-bit **checksum** , but the size of this field can be negotiated. LCP is used to establish, configure, and **test** the integrity of the data-link connection. LCP allows negotiating various parameters dynamically, including whether...

18/3,K/45 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04454329 Supplier Number: 56194010 (USE FORMAT 7 FOR FULLTEXT)
TOSHIBA: Toshiba participates in TELECOM 99 in Ge Geneva.
M2 Presswire, pNA
Oct 8, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 823

... with a self-healing function.
Multi Protocol Label Switching (MPLS)
A key technology for Dynamic **VPN** , MPLS achieves extremely high packet transfer speeds. Every packet in the network is assigned a...

...route separately from transfer processing. The label eliminates the extra load created by having to **examine** the **IP header** .
Infrastructure Access
Broadband Wireless Access System
As a "last mile" solution, broadband wireless access systems...
?

```
File 256:SoftBase:Reviews,Companies&Prods. 82-2004/Feb
         (c)2004 Info.Sources Inc
File   2:INSPEC 1969-2004/Mar W1
         (c) 2004 Institution of Electrical Engineers
File   6:NTIS 1964-2004/Mar W1
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2004/Mar W1
         (c) 2004 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Mar W1
         (c) 2004 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2004/Feb
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/Mar W2
         (c) 2004 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2004/Mar W1
         (c)2004 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2004/Feb W4
         (c) 2004 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Feb
         (c) 2004 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2004/Mar 15
         (c) 2004 The Gale Group
File 144:Pascal 1973-2004/Mar W1
         (c) 2004 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2004/Feb 27
         (c) 2004 EBSCO Publishing
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File 266:FEDRIP 2004/Jan
         Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2004/Mar 12
         (c) 2004 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 603:Newspaper Abstracts 1984-1988
         (c)2001 ProQuest Info&Learning

Set     Items   Description
S1      34097   TTL OR TTF OR TIME(1W)(LIVE OR LIFE)
S2        744   (HOP OR HOPS)(2N)(LIMIT??? ? OR LIMITATION? OR COUNT??? ? -
                 OR ALLOW?)
S3        817   (IP OR INTERNET OR PROTOCOL OR ICMP OR DNS)(1W)(FIELD? ? OR
                 HEADER? ?)
S4     467452   TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S5       2159   IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5 OR SOCKS(-
                 )V5 OR LAYER()(TWO OR 2)()FORWARD??? ? OR L2F
S6       9844   VPN OR VPNS OR VIRTUAL()PRIVATE()(NET OR NETWORK? ?)
S7     665998   ENCAPSULAT? OR WRAP???? ? OR INSULAT?
S8       3534   (SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHE-
                 R?)(2N)(CONNECT???? ? OR CONNECTIVIT? OR CHANNEL? ? OR PATH? ?
                 OR PATHWAY? OR PASSAGE? ?)
S9      20522   (SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHE-
                 R?)(2N)(COMMUNICAT???? ? OR ACCESS OR ACCESS?? ? OR ACCESSING)
S10     14969   PRIVATE(1W)(NET OR NETS OR NETWORK?)
S11  13233746   VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALIDAT? OR CHEC-
                 K??? ? OR CHEQU? OR EXAMIN? OR TEST OR TESTS OR TESTED OR TES-
                 TING? OR EVALUAT? OR CONFIRM?
S12     68619   AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CRO-
                 SSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQU?
```

S13 3012 S1:S3 AND S4:S10
S14 432 S13 AND S11:S12
S15 129961 S4:S10(15N)S11:S12
S16 124 S14 AND S15
S17 2945 S1:S2 AND S4:S10
S18 414 S17 AND S11:S12
S19 24 S16/2001:2004
S20 87 S16 NOT (S19 OR WIND()TUNNEL? OR DIODE? OR LOGIC OR TRANSI-STOR? OR TUNNEL()BAT)
S21 56 RD (unique items)
S22 32 S21 NOT BEDT

22/7/1 (Item 1 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00106386 DOCUMENT TYPE: Review

PRODUCT NAMES: IPSec **(836796**

TITLE: Authentication **Encryption: Bulletproof IP**
AUTHOR: Thayer, Rodney
SOURCE: Data Communications, v26 n16 p54(6) Nov 21, 1997
ISSN: 0363-6399

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

IETF's **IPSec** , a group of security protocols that add **authentication** and encryption to all Internet Protocol (IP) communications, is described in detail. As with IP, **IPSec** is flexible, with **authentication** features that allow network managers to protect against attacks coming from inside or outside the network. Encryption prevents hackers from decoding packets as they navigate links. This is important for companies that wish to create connections to trading partners, suppliers, or customers via the Internet. Managers also can select the type of encryption to be used. TCP/IP is highly extensible and allows new services to be layered over an existing framework. A standard packet has an **IP header** , with a source and destination address, control fields, and information about the packet contents. One control field is a 'next **protocol** ' **field** that specifies what will follow the header. The next protocol is generally TCP or UDP in the instance of IP packets, but it could be another protocol. **IPSec** adds new fields to packet headers, which make **authentication** and encryption possible. **IPSec** protocols **validate** packets with a secret key that the receiver and sender share. **IPSec** 's protocols include **encapsulating** security payload, **authentication** header, and **IP security** association key management protocol.

REVISION DATE: 20010730

22/7/2 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6805867 INSPEC Abstract Number: B2001-02-6150M-068
Title: Characterization of performance of TCP/IP over PPP and ATM over asymmetric links
Author(s): Phanse, K.S.; DaSilva, L.A.; Kidambi, K.

Author Affiliation: Bradley Dept. of Electr. Eng., Virginia Polytech. Inst. & State Univ., Alexandria, VA, USA
Conference Title: Proceedings Ninth International Conference on Computer Communications and Networks (Cat.No.00EX440) p.334-9
Editor(s): Engbersen, T.; Park, E.K.
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 2000 Country of Publication: USA xxii+661 pp.
ISBN: 0 7803 6494 5 Material Identity Number: XX-2000-02515
U.S. Copyright Clearance Center Code: 0 7803 6494 5/2000/$10.00
Conference Title: Proceedings Ninth International Conference on Computer Communications and Networks
Conference Sponsor: Army Res. Lab.; IBM; Nokia; Telcordia; IEEE Commun. Soc
Conference Date: 16-18 Oct. 2000 Conference Location: Las Vegas, NV, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P); Theoretical (T)
Abstract: The objective of this paper is to characterize and analyze the performance of TCP/IP when used over point-to-point protocol (PPP) and asynchronous transfer mode (ATM) on asymmetric links. This will allow us to gain insight into this new protocol architecture used in the asymmetric digital subscriber line (ADSL) access network and to investigate the related quality of service (QoS) issues. Using simulation, we **verified** the effects of asymmetry on the performance of TCP and additional throughput degradation caused by segmentation at the ATM layer. This study was done for unidirectional and bidirectional data transfer using different traffic mixes. We also quantified the improvement in the downstream throughput obtained by delaying the TCP acknowledgements and using TCP/ **IP header** compression. Although these techniques are effective for unidirectional TCP/IP data transfer over asymmetric links, they do not prove as effective for bidirectional traffic, and the problem further exacerbates when ATM enters the scenario. Hence, there is a need for additional enhancements in such scenarios. Further, we modified the existing protocol stack model to implement PPP **encapsulation** over the ATM adaptation layer (AAL5). We characterized and analyzed the effect of the additional PPP overhead on system performance in terms of throughput degradation and additional delay. We also **evaluated** the use of TCP/ **IP header** compression for improving performance in presence of PPP **encapsulation** . (10 Refs)
Subfile: B

22/7/20 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05129805 E.I. No: EIP98104402301
Title: Understanding and implementing effective VPNs
Author: LaBorde, Doug
Corporate Source: Ascend Communications Inc, Alameda, CA, USA
Source: Storage Management Solutions v 3 n 2 Mar 1998. 4p
Publication Year: 1998
CODEN: SMSOFD
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)
Journal Announcement: 9811W5
Abstract: The many advantages of **virtual private networks** (**VPN**) make enterprise networking over public data networks inevitable. Essentially, a **VPN** allows organizations to use a public data network,

such as the Internet, securely enough for some or all of the enterprise WAN communications needs. There are compelling reasons for replacing private links utilizing the voice-oriented public switched telephone network with **VPNs** that utilize a public data network instead. **VPNs** require less equipment and fewer lines than **private networks** , and are less of a management burden, particularly when remote user support is outsourced to Internet service providers.

22/7/29 (Item 1 from file: 95)

01180775 E98020307351
Security Solutions
Boss, A
Datrac Laupen, CH
M+K Computermarkt, v20, n2, pp56-58, 1998
Document type: journal article Language: German
Record type: Abstract
ISSN: 1420-5068

ABSTRACT:
Im Zuge der rasant zunehmenden Globalisierung und dem daraus resultierenden Konkurrenzdruck ist es notwendig geworden, selbst extrem sensitive Daten immer schneller uebertragen zu koennen. Hinzu kommt der Electronic Commerce, der ebenfalls die unbedingte Integritaet von Informationen erfordert. Bei der Planung einer Sicherheitspolitik fuer unternehmensweite Wide Area Networks (WAN) unterscheidet man zwei Elemente: Die Identitaet des Benutzers und die Integritaet der Daten und der Infrastruktur. Die Identitaet wird durch die Anwendung einer Policy erreicht, Datenintegritaet durch Datenverschluesselung. Auf OSI-Ebene sind es drei Schichten, die fuer die Datenverschluesselung in Frage kommen: Physical & Link-Layer, Network Layer und Application Layer. Die Firma Cisco Systems unterstuetzt softwareseitig auf ihren Routern den Data Encryption Standard (DES), der im Artikel kurz beschrieben wird. Mit Hilfe des von Microsoft in diesem Jahr bei Windows 98 und NT 5.0 erstmalig implementierten **IP Security** (**IPsec**) wird es moeglich sein, Nachrichten unabhaengig vom OSI-Layers und des Verschluesselungsalgorithmus zu chiffrieren. Durch die zwei neuen Header **Authentication** Header (AH) und **Encapsulating** Payload Header (ESP), die hinter dem eigentlichen **IP - Header** eingefuegt werden, wird sowohl IPv4 als auch IPv6 um ein leistungsfaehiges Merkmal erweitert. Dabei wird das Internet Security and Key Management Protocol (ISAKMP) eines der neuen Schluesselmanagement-Protokolle sein, das in Kooperation mit **IPsec** verwendet wird. Durch AH und ESP wird es moeglich, einen gesicherten Kommunikationskanal zwischen Sender und Empfaenger aufzubauen. ISAKMP dient dazu, die Sicherheitswerte fuer diesen Kanal zu ermitteln und die notwendigen Schluessel auszutauschen.
?

(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10428

English Abstract
A mobile node may roam away from its home network to a foreign network. The mobile node may communicate using the Mpbile Internet Protocol, and it may use Internet Protocol security to communicate with its home network. A foreign agent on the foreign network and a home agent on the home network may dynamically link a policy to be used for a Internet Protocol security session between the foreign agent and the home agent. The foreign agent and the home agent may dynamically create a filter to be used for the Internet Protocol Security session.

French Abstract
Selon l'invention, un noeud mobile peut realiser une itinerance a distance de son reseau mere vers un reseau etranger. Le noeud mobile peut communiquer au moyen du protocole Internet mobile et utiliser un protocole de securite Internet pour communiquer avec son reseau mere. Un agent relais sur le reseau etranger et un agent mere sur le reseau mere peuvent realiser l'association dynamique d'une regle a utiliser pour une session de protocole de securite Internet entre l'agent relais et l'agent mere. L'agent relais et l'agent mere peuvent creer dynamiquement un filtre a utiliser pour la session de protocole de securite Internet.

Legal Status (Type, Date, Text)
Publication 20031030 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Detailed Description
Detailed Description

26/5,K/8 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01057878 **Image available**
PROCESSING A PACKET USING MULTIPLE PIPELINED PROCESSING MODULES
TRAITEMENT DE PAQUET AU MOYEN DE MODULES DE TRAITEMENT PIPELINES MULTIPLES
Patent Applicant/Assignee:
HI FN INC, 750 University Avenue, Los Gatos, CA 95032-7695, US, US (Residence), US (Nationality)
Inventor(s):
SAVARDA Raymond, 4224 Sancroft Drive, Apex, NC 27502, US,
BLAKER David, 109 Hogan Glen Court, Chapel Hill, NC 27516, US,
WINKELSTEIN Dan, 2308 Lawrence Drive, Raleigh, NC 27603, US,
Legal Representative:
MYERS BIGEL SIBLEY & SAJOVEC P A (agent), P.O. Box 37428, Raleigh, NC 27627, US,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200388072 A1 20031023 (WO 0388072)
Application: WO 2003US10545 20030408 (PCT/WO US0310545)
Priority Application: US 2002120577 20020411
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G06F-015/80**
International Patent Class: H04L-012/56; H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 11500

English Abstract
A packet is processed by encapsulating the packet with a packet-object header if the packet does not have a packet-object header. The encapsulated packet is processed based on information contained in the packet-object header using a plurality of transform modules that are coupled to each other in a series or pipeline configuration. The plurality of transform modules process the encapsulated packet independent of each other.

French Abstract
Selon l'invention, un paquet est traite par encapsulation avec un en-tete d'objets de paquet si ledit paquet ne comporte pas d'en-tete d'objets de paquet. Le paquet encapsule est traite en fonction d'informations contenues dans ledit en-tete d'objets de paquet, au moyen d'une pluralite de modules de transformation couples les uns aux autres en serie ou selon une configuration pipeline. La pluralite de modules de transformation traite les paquets encapsules, independamment les uns des autres.

Legal Status (Type, Date, Text)
Publication 20031023 A1 With international search report.
Publication 20031023 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20031224 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **G06F-015/80**
Fulltext Availability:
Detailed Description
Detailed Description
... 108 may be configured to determine if the packet-object is to be subject to **IPSec** transforms by **examining** the **IP header protocol field** . If the **IP header protocol field** is ESP or AH, then the destination IP address is compared with valid destination IP...

...SAD lookup module 118.

The outbound pre-crypto module 122 may be configured to handle **time** -to-**live** (**TTL**) decrement operations, pre-cryptographic fragmentation, and insertion of **IPSec** information into the crypto header 215. In more

detail, the outbound pre-crypto module 122 may **check** a forwarded flag in the pipeline processing header 205 to determine whether a packet-object...

...the packet-object. The outbound pre-crypto module 122 may obtain the keys (encryption and **authentication**), sequence number, and outer **IP header** (for **tunnel** mode) from the SAD database. This information may be formatted in various ways, in accordance

26/5,K/9 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01033401 **Image available**
METHOD AND SYSTEM FOR SENDING A MESSAGE THROUGH A SECURE CONNECTION
PROCEDE ET SYSTEME D'ENVOI D'UN MESSAGE PAR UNE CONNEXION SECURISEE
Patent Applicant/Assignee:
INTRASECURE NETWORKS OY, PL 38, FIN-02201 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
VAARALA Sami, Neljas Linja 22 A, FIN-00530 Helsinki, FI, FI (Residence), FI (Nationality), (Designated only for: US)
NUOPPONEN Antti, Kaksoiskiventie 7-9 A 1, FIN-02760 Espoo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
INNOPAT LTD (agent), P.O. Box 556, FIN-02151 Espoo, FI,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200363443 A1 20030731 (WO 0363443)
Application: WO 2003FI45 20030121 (PCT/WO FI0300045)
Priority Application: FI 2002112 20020122
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
International Patent Class: H04Q-007/38
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 13623

English Abstract
The method and system of the invention enable secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network. It is mainly characterized in that a message is formed in the first computer or in a computer that is served by the first computer, and in the latter case, sending the message to the first computer. In the first computer, a secure message is then formed by giving the message a unique identity and a destination address. The message is sent from the first computer to the intermediate computer, whereafter said destination address and the unique identity are used to find an address to the second computer. The current destination address is substituted with the found address to the second computer, and the

unique identity is substituted with another unique identity. Then the message is forwarded to the second computer.

French Abstract
L'invention concerne un procede et un systeme qui permettent d'envoyer de maniere securisee un message a partir d'un premier ordinateur vers un second ordinateur par le biais d'un ordinateur intermediaire sur un reseau de telecommunications. Lesdits procede et systeme se caracterisent principalement en ce qu'un message est forme dans le premier ordinateur ou dans un ordinateur servi par le premier ordinateur et, en l'occurrence, ledit ordinateur envoie le message au premier ordinateur. Dans le premier ordinateur, on forme un message securise en lui donnant une identite unique et une adresse de destination. Le message est envoye du premier ordinateur vers l'ordinateur intermediaire; lesdites adresse de destination et identite unique sont ensuite utilisees pour trouver une adresse au second ordinateur. L'adresse de destination en cours est remplacee par l'adresse trouvee pour le second ordinateur, et l'identite unique par une autre identite unique. Le message est alors envoye au second ordinateur.

Legal Status (Type, Date, Text)
Publication 20030731 A1 With international search report.
Publication 20030731 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20031016 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... packet is identical to the one used by the first computer for the AH integrity **check** value calculation, except possibly for fields not covered by. AH (such as.- the- **Time** -Tom- **Live** field, the- header checksurrL etc). Thus, the AH integrity **check** value is now correct.

In step 3, the second computer performs standard **IPSec** processing of AH. The packet, which now is uncovered from the tunnel is sent to...

26/5,K/10 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01028881 **Image available**
METHODS AND APPARATUS FOR ENCAPSULATING A FRAME FOR TRANSMISSION IN A STORAGE AREA NETWORK
PROCEDES ET APPAREILS D'ENCAPSULATION D'UNE TRAME EN VUE DE SA TRANSMISSION DANS UN RESEAU DE STOCKAGE
Patent Applicant/Assignee:
ANDIAMO SYSTEMS INC, 375 East Tasman Drive, San Jose, CA 95134, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
EDSALL Thomas James, 13208 Peacock Court, Cupertino, CA 95014, US, US (Residence), US (Nationality), (Designated only for: US)
DUTT Dinesh Ganapathy, 1176 Corral Ave., Sunnyvale, CA 94086, US, US (Residence), IN (Nationality), (Designated only for: US)
GAI Silvano, 3021 Mauna Loa Ct., San Jose, CA 95132, US, US (Residence), IT (Nationality), (Designated only for: US)

Legal Representative:
HEILBRUNN ELISE R (agent), Beyer Weaver & Thomas LLP, P.O. Box 778, Berkeley, CA 94704, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200358891 A1 20030717 (WO 0358891)
Application: WO 2002US41072 20021223 (PCT/WO US0241072)
Priority Application: US 200134160 20011226
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/46
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9093

English Abstract
Methods and apparatus for encapsulating a packet or frame for transmission in a storage area network are disclosed. A packet or frame compatible with a standard protocol employed in the storage area network is received or generated. The packet or frame is then encapsulated with a virtual storage area network identifier. The packet or frame may further be encapsulated with at least one of a TTL value, MPLS information, and a type of traffic to be carried by the packet or frame. For instance, the type of traffic to be carried by the packet or frame may include Ethernet, Fibre Channel, and Infiniband. Once encapsulated, the encapsulated packet or frame is sent over the storage area network. For instance, the encapsulated packet or frame may be generated as well as transmitted by a switch over an inter-switch link in the storage area network.

French Abstract
L'invention concerne des procedes et des appareils d'encapsulation d'un paquet ou d'une trame en vue de sa transmission dans un reseau de stockage. Un paquet ou une trame compatible avec un protocole standard utilise dans le reseau de stockage est recu(e) ou genere(e). Le paquet ou trame est ensuite encapsule(e) avec un identificateur de reseau de stockage virtuel, puis avec au moins une valeur TTL, une information MPLS et un type de trafic pris en charge par le paquet ou la trame. Par exemple, le type de trafic que le paquet ou la trame peut prendre en charge peut comprendre Ethernet, Fibre Channel et Infiniband. Une fois encapsule(e), le paquet ou la trame est envoye(e) via le reseau de stockage. Le paquet ou la trame encapsule(e) peut, par exemple, etre genere(e) et transmis(e) par un commutateur via une liaison intercommutateur dans le reseau de stockage.

Legal Status (Type, Date, Text)
Publication 20030717 A1 With international search report.
Publication 20030717 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20031023 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims

Claim
... value and the MPLS information.

4 The method as recited in claim 1, wherein the **TTL** value specifies a number of remaining hops that can be traversed before the **encapsulated** packet or frame is dropped.

5 The method as recited in claim 1, wherein the **TTL** value specifies a remaining lifetime.

6 The method of claim 3, further comprising calculating an error **check** value for the new packet or frame and including the error check value in the...the MPLS information.

25 The computer-readable medium as recited in claim 22, wherein the **TTL** value specifies a number of remaining hops that can be traversed before the **encapsulated** packet or frame is dropped.

26 The method as recited in claim 22, wherein the **TTL** value specifies a
remaining lifetime. - 27
. The computer-readable medium of claim 24, further comprising instructions for calculating an error **check** value for the new packet or frame and including the error check value in the...

26/5,K/11 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01019348 **Image available**
METHOD AND APPARATUS FOR MANAGING CONGESTION IN A DATA COMMUNICATION NETWORK
PROCEDE ET APPAREIL PERMETTANT DE GERER UNE CONGESTION DANS UN RESEAU DE COMMUNICATION DE DONNEES
Patent Applicant/Assignee:
MOTOROLA INC, 1303 East Algonquin Road, Schaumburg, IL 60196, US, US (Residence), US (Nationality)
Inventor(s):
LUTGEN Craig L, 3212 Thorne Hill Court, Richardson, TX 75082, US,
RAY Dale E, 6217 Riverview Circle, Fort Worth, TX 76112, US,
Legal Representative:
MAY Steven A (et al) (agent), Motorola, Inc., Intellectual Property Dept., 1303 East Algonquin Road, Schaumburg, IL 60196, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200349387 A1 20030612 (WO 0349387)
Application: WO 2002US34476 20021028 (PCT/WO US0234476)
Priority Application: US 2001999118 20011130
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/56

International Patent Class: H04L-012/28
Publication Language: English
Filing Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 6686

English Abstract
  A communication system manages data congestion and/or contention occurring at a point-of-traffic concentration by reading (504) a time value associated with a data packet, the time value being representative of when the data packet entered the network. The time value is within the header of the data packet. The age of the data packet is determined (506) from the time value. The data packet is discarded (508) if the age of the data packet is above a threshold value. Alternatively, a first time value determined from a time reference is associated (404) with a data packet at a first node. The data packet is transmitted to a second node and the first time value is compared (506) to a second time value to provide a result. The second time value is also determined from the time reference. The data packet is discarded (508) if the result exceeds a threshold value.

French Abstract
  Un systeme de communications gere une congestion et/ou une contention de donnees au niveau d'un point de concentration de trafic par lecture (504) d'une valeur temporelle associee a un paquet de donnees, ladite valeur temporelle etant representative du moment ou ledit paquet de donnees entre dans un reseau. La valeur temporelle se trouve dans l'en-tete du paquet. L'age du paquet de donnees est determine (506) a partir de cette valeur temporelle. Le paquet de donnees est supprime (508) lorsque l'age du paquet de donnees est superieur a une valeur seuil. Dans un autre mode de realisation, une premiere valeur temporelle determinee a partir d'une reference temporelle est associee (404) a un paquet de donnees au niveau d'un premier noeud. Ledit paquet de donnees est ensuite transmis a un second noeud et la premiere valeur temporelle est comparee (506) a une seconde valeur temporelle afin d'obtenir un resultat. La seconde valeur temporelle est egalement determinee a partir de la reference temporelle. Ledit paquet de donnees est supprime (508) lorsque le resultat est superieur a une valeur seuil.

Legal Status (Type, Date, Text)
Publication 20030612 A1 With international search report.
Publication 20030612 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20030814 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
  Detailed Description

Detailed Description
... The Fragment Offset 322 is used to direct the reassembly of a fragmented datagram. The **Time** -To- **Live** field 3 1 0 was described above as a counter ineremenling in either seconds or in hopcounts. The Protocol 326 specifies the next **encapsulated** protocol (e.g., IPv6 Hop-by-Hop Option, Internet Control Message Protocol, Internet Group Multicast Protocol, RSVP Reservation Protocol, etc.). The **Checksum** 328 **verifies** the header by detecting effors using a one's complement of the

IP header and...

26/5,K/12 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00967925 **Image available**
METHOD AND SYSTEM FOR HIGH-SPEED PROCESSING IPSEC SECURITY PROTOCOL PACKETS
PROCEDE ET SYSTEME POUR LE TRAITEMENT A GRANDE VITESSE DES PAQUETS DE PROTOCOLE DE SECURITE IPSEC

Patent Applicant/Assignee:
CORRENT CORPORATION, 1711 West Greentree Drive, Suite 201, Tempe, AZ 85283, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
NOEHRING Lee P, 22415 North 67th Drive, Glendale, AZ 85310, US, US (Residence), US (Nationality), (Designated only for: US)
MERCER Chad W, 287 East Hampton Lane, Gilbert, AZ 85296, US, US (Residence), US (Nationality), (Designated only for: US)
CASSETTI David, 1251 East Loius Way, Temple, AZ 85284, US, US (Residence), US (Nationality), (Designated only for: US)
PRIVETT Michael, 879 West Tremaine Avenue, Gilbert, AZ 85233, US, US (Residence), US (Nationality), (Designated only for: US)
ANAND Satish, 1223 East Saragosa Street, Chandler, AZ 85225, US, US (Residence), IN (Nationality), (Designated only for: US)
Legal Representative:
STEFFEY Charles E (et al) (agent), Schwegman, Lundberg, Woessner & Kluth, P.O. Box 2938, Minneapolis, MN 55402, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 2002102026 A2 20021219 (WO 02102026)
Application: WO 2002US19079 20020612 (PCT/WO US0219079)
Priority Application: US 2001297646 20010612; US 2001880701 20010613
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
International Patent Class: H04L-012/28
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10932

English Abstract
A packet processing system is embodied on an ASIC is optimized for processing IPSec security protocol packets in a hardware configuration. Embedded RISC processors operate with hardware support modules providing for IPSec packet processing at OC24 data rates and greater. IPSec packets are received through a streaming interface and buffered in an external memory. When the entire packet is in external memory, portions are buffered in a local memory for cryptoprocessing. As portions of the packets complete processing, the portions are buffered to an output portion of the external memory associated with the channel. When an entire packet competes processing, portions are buffered to a local memory for streaming. The hardware accordingly reduces the involvement of

the RISC processors and significantly increases channel throughput providing for high-speed IPSec packet processing.

French Abstract
L'invention concerne un systeme de traitement de paquets fonctionnant sur circuit integre specifique, optimise pour le traitement des paquets de protocole de securite IPSec dans une configuration de materiel. Aux fins de l'invention, des processeurs RISC integres fonctionnent avec des modules de soutien pour le materiel, assurant le traitement des paquets IPSec a des debits binaires OC24 ou superieurs. Les paquets IPSec sont recus via une interface de flux et font l'objet d'un tamponnage dans une memoire externe. Pour chaque paquet entier memorise dans la memoire externe, des parties de paquet font l'objet d'un tamponna
ge dans une memoire locale, aux fins de cryptotraitement. A mesure qu'elles sont traitees, ces parties font l'objet d'un tamponnage en zone de sortie dans la memoire externe associee au canal. Lorsqu'un paquet entier arrive en fin de traitement, des parties de paquet font l'objet d'un tamponnage en memoire locale pour incorporation au flux. Dans ces conditions, le materiel reduit la participation des processeurs RISC et augmente considerablement le debit sur canal en assurant un traitement de paquets IPSec a grande vitesse.

Legal Status (Type, Date, Text)
Publication 20021219 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Claims

Claim
... the IP data packet.
35 The method as claimed in claim 26 further comprises
5 **checking** a path maximum transmission unit (PMTU) value of the IP data packet including the security header and the outer **IP header** as prepended
to the IP data packet to determine when the PMTU value exceeds a PMTU value for a **tunnel** through which the security protocol data packet is destined.
3 9
. The method as claimed...

26/5,K/13 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00955248 **Image available**
IP SECURITY AND MOBILE NETWORKING
SECURITE IP ET MISE EN RESEAU MOBILE
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality)
Inventor(s):
HAVERINEN Henry, Arkkitehdinkatu 15 A 3, FIN-33720 Tampere, FI,
HONKANEN Jukka-Pekka, Pyynikintie 23 A 13, FIN-33230 Tampere, FI,
KUIKKA Antti, Sontulantie 324, FIN-37800 Toijala, FI,
Legal Representative:
JOHANSSON Folke (agent), c/o Nokia Corporation, P.O. Box 226, FIN-00045 Nokia Group, FI,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200289395 A1 20021107 (WO 0289395)

Application: WO 2002FI293 20020405 (PCT/WO FI0200293)
Priority Application: FI 2001876 20010426
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-009/00**
International Patent Class: H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 5772

English Abstract
The invention discloses a method transferring packets between a mobile host device (100) and a source node via a number of independent data networks while maintaining a secure connection. The independent networks may include, for example, the Internet (120), localized Access Zones (110,140), a Corporate Intranets, a Home Network (130) etc. Problems may occur, for example, when the mobile node is using a co-located care-of address, in which case both IP-in-IP and IPsec tunneling transformations are performed, and the current IPsec and IP-in-IP implementations cannot perform the required tunneling operations on the mobile host. This is because the IP-in-IP and IPsec tunneling when the IP-in-IP tunnel is not the outermost transformation. In an embodiment of the invention, the security policy operated by the mobile host includes a primary security policy and a dynamic secondary security policy that selectively apply specified transformations to certain packets in the data transfer.

French Abstract
L'invention concerne un procede destine a transferer des paquets entre un dispositif hote mobile (100) et un noeud source par l'intermediaire d'une pluralite de reseaux de donnees independants tout en assurant le maintien d'une connexion securisee. Les reseaux independants peuvent comprendre, par exemple, Internet (120), des zones d'acces localisees (110, 140), des reseaux intranet d'entreprises, un reseau domestique (130), etc. Des problemes peuvent survenir, par exemple, lorsque le noeud mobile utilise une adresse temporaire colocalisee, d'ou la realisation des transformations de tunnellisation IP dans IP et IPsec, les implementations IPsec et IP dans IP en cours ne pouvant pas executer les operations de tunnellisation sur l'hote mobile. Cela est du a la tunnellisation IP dans IP et IPsec lorsque le tunnel IP dans IP n'est pas la transformation la plus a l'exterieur. Dans un mode de realisation de l'invention, la regle de securite mise en oeuvre par l'hote mobile comprend une regle de securite principale et une regle de securite secondaire dynamique permettant d'appliquer selectivement des transformations specifiees sur certains paquets dans le transfert de donnees.

Legal Status (Type, Date, Text)
Publication 20021107 A1 With international search report.
Examination 20030103 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **H04L-009/00**

Fulltext Availability:
Detailed Description

Detailed Description
... to a number of security policies from associated networks. The outermost transformation is the AH **tunnel** 104 of figure 1 comprising the **IP header** 300 between the terminal's current care-of address and the PAC. Inside the AH **tunnel** 305, there is an IP-in-1P **tunnel** of Mobile IP between the terminal's current care-of address and the home agent (HA) that comprises **IP header** 310. The AH may include processes such as **check** sum and **authentication** codes for ensuring packet security.

Furthermore, inside the IP-in-IP **tunnel** there is the **VPN tunnel** between the terminal's home address and the **VPN** gateway that comprises **IP header** 320. Inside the **VPN tunnel** , there is the original IP packet comprising header 330 and payload 340 that is transmitted... security associations) and their order of application are kept track of. In step 805, a **check** is made for any remaining **IPSec** and/or IP-in- **IP headers** , if there are, the inbound SAD lookup of step 807 is repeated. If not, the...

26/5,K/14 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00918709 **Image available**
PACKET ENCRYPTON SYSTEM AND METHOD
SYSTEME ET PROCEDE DE CRYPTAGE DE PAQUETS
Patent Applicant/Assignee:
MOSAID TECHNOLOGIES INCORPORATED, 11 Hines Road, Kanata, Ontario K2K 2X1, CA, CA (Residence), CA (Nationality)
Inventor(s):
LOW Arthur John, 5 Carman Road, Chelsea, Quebec J9B 2K3, CA,
DAVIS Stephen J, 14 Wiltshire Circle, Nepean, Ontario K2J 4L1, CA,
Legal Representative:
FREEDMAN Gordon (agent), Freedman & Associates, 117 Centrepointe Drive, Suite 350, Nepean, Ontario K2G 5X3, CA,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200252777 A2-A3 20020704 (WO 0252777)
Application: WO 2001CA1858 20011221 (PCT/WO CA0101858)
Priority Application: US 2000741829 20001222
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-009/00**
International Patent Class: H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 7437

English Abstract
A processor has an input port for receiving packets of data to be processed for encryption. A master controller acts to analyse the packets and to provide a header including a list of processes to perform on the packet of data and an ordering thereof. The master controller is programmed with process related data relating to the overall processing function of the processor. The header is appended to the packet of data. the packet with the appended header information is stored within a buffer. A buffer controller acts to dtermine for each packet stored within the buffer based on the header within the packet a next processor to process the packet. The controller then provides the packet to the determined processor for processing. The processed packet is returned with some indication that the processing is done. For example, the process may be deleted from the list of processes. The buffer controller repeatedly makes a determination of a next process until there is no next process for a packet at which time it is provided to an output port.

French Abstract
Cette invention concerne un processeur possedant un port d'entree pour la reception de paquets de donnees destines a etre traites pour cryptage. Un controleur principal analyse les paquets et fournit une en-tete renfermant une liste d'operations a effectuer sur les paquets des donnees et un classement de ces derniers. Ce controleur principal est programme avec des donnees de processus en rapport avec la fonction de traitement globale du processeur. L'en-tete est annexee au paquet de donnees. Le paquet de donnees avec en-tete annexee est stocke dans une memoire tampon. Un controleur de memoire tampon sert a determiner le processeur suivant pour le traitement du paquet, ceci pour chaque paquet stocke dans la memoire tampon en fonction de l'en-tete qui lui est annexee. Le controleur transmet ensuite le paquet au processeur retenu pour traitement. Apres traitement, le paquet revient assorti d'une quelconque indication que le traitement a ete execute. Par exemple, l'operation peut etre supprimee de la liste des operations. Le controleur de memoire tampon determine l'etape suivante jusqu'a ce que les etapes soient epuisees pour un paquet, lequel est alors transmis au port de sortie.

Legal Status (Type, Date, Text)
Publication 20020704 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20020926 Late publication of international search report
Republication 20020926 A3 With international search report.
Republication 20020926 A3 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20021219 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... processed in at least one of the processors, and it may include an encryption or **authentication** key. Individual processors may also add result data to the control data.

The processors may perform **IPSEC** protocol processing including **IP header** manipulation, encryption, and **authentication** . Other processes such as

SSL protocol processes may also be performed.

hi accordance with certain...

Claim
... 7 The system as claimed in any of Claims 1-6 wherein the processors perform **IPSEC** protocol processing.
1 7
. A system as claimed in any of Claims 1-7 wherein respective processors perform **IP** **header** manipulation and encryption.

9 A system as claimed in any of Claims 1-8 wherein a processor performs **authentication** processing.

10 A method of encrypting or decrypting data packets comprising:
modifying a received packet...

...The method as claimed in any of Claims 10- 1 6 wherein the processors perform **IPSEC** protocal processing.

18 A method as claimed in any of Claims 10- 17 wherein respective processors perform **IP** **header** manipulation and encryption.

19 A method as claimed in any of Claims 10- 1 8 wherein a processor performs **authentication** processing.
20 A data processor for processing data comprising:
an input port for receiving packets...

26/5,K/15 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00916586 **Image available**
INTEGRATED INTELLIGENT INTER/INTRA-NETWORKING DEVICE
DISPOSITIF INTELLIGENT INTEGRE D'INTER/INTRARESEAUTAGE
Patent Applicant/Assignee:
SOORIYA NETWORKS INC, 600 Meridian Avenue, Suite 100, San Jose, CA 951126 , US, US (Residence), US (Nationality)
Inventor(s):
VAIRAVAN Kannan P, 7625 Westhill Lane, Cupertino, CA 95014, US,
Legal Representative:
NORTH Michael V (et al) (agent), Fenwick & West Llp, Two Palo Alto Square, Palo, Alto CA 94306, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200250680 A1 20020627 (WO 0250680)
Application: WO 2001US50023 20011220 (PCT/WO US0150023)
Priority Application: US 2000258156 20001221; US 2001894224 20010627
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-011/30
International Patent Class: G06F-012/14; **G06F-015/16** ; **G06F-015/173** ; **H04L-009/00** ; **H04L-009/32**
Publication Language: English

Filing Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 12566

English Abstract
  An integrated, easily upgradeable networking device (110) capable of interfacing with different types of networks (105a, 105b, 105c, 105d) while still providing high performance networking functionalities such as protocol conversion, security maintenance, and inter/intra-network management within an enterprise environment is described. The device (110) may perform various networking functions within an enterprise and is easily adaptable to perform both inter-networking functions as well as intra-networking functions.
French Abstract
  L'invention concerne un dispositif de reseautage integre (110) facilement extensible pouvant faire interface avec differents types de reseaux (105a, 105b, 105c, 105d) tout en conservant des fonctionnalites de reseautage a hautes performances, notamment en termes de conversion de protocole, de maintien de securite et de gestion d'interreseau/intrareseau dans un environnement d'entreprise. Ce dispositif (110) peut executer diverses fonctions de reseautage au sein d'une entreprise. Il est facilement adaptable en vue de l'execution de fonctions d'interreseautage ou d'intrareseautage.

Legal Status (Type, Date, Text)
Publication 20020627 A1 With international search report.
Publication 20020627 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Correction 20031009 Corrected version of Pamphlet: pages 32-35, claims, replaced by new pages 32-35; due to late transmittal by the receiving Office
Republication 20031009 A1 With international search report.

...International Patent Class: **G06F-015/16** ...
... **G06F-015/173** ...

... **H04L-009/00** ...

... **H04L-009/32**
Fulltext Availability:
  Claims

Claim
... the packet processor comprises a virtual private network policy and table module for implementing a **virtual private network** .

13 The device of claim 12 wherein the **virtual private network** policy and table module
comprises:
an **Internet Protocol header authentication** module for providing connectionless
integrity and data origin for Internet Protocol data packets;
an **encapsulated** security payload module for conveying encrypted data in an
Internet Protocol datagram; and
an encryption...

26/5,K/16 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00905538 **Image available**
A METHOD FOR SECURE PACKET-BASED COMMUNICATION BETWEEN TWO UNITS VIA AN INTERMEDIA UNIT
PROCEDE PERMETTANT DE TRANSMETTRE DE MANIERE SURE DES DONNEES EN PAQUETS ENTRE DEUX UNITES VIA UNE UNITE INTERMEDIAIRE

Patent Applicant/Assignee:
ICOMERA AB, Stena Center 1C, S-412 92 Goteborg, SE, SE (Residence), SE (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
BERGEK Martin, Kullengatan 8B, S-412 62 Goteborg, SE, SE (Residence), SE (Nationality), (Designated only for: US)
HOJLUND Mats, Krokslatts Parkgata 67 A, S-431 68 Moldal, SE, SE (Residence), SE (Nationality), (Designated only for: US)
Legal Representative:
AWAPATENT AB (agent), Box 11394, S-404 28 Goteborg, SE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200239657 A1 20020516 (WO 0239657)
Application: WO 2001SE2462 20011108 (PCT/WO SE0102462)
Priority Application: SE 20004076 20001108
Designated States: AE AG AL AM AT AT (utility model) AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ CZ (utility model) DE DE (utility model) DK DK (utility model) DM DZ EC EE EE (utility model) ES FI FI (utility model) GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SK (utility model) SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-009/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4518

English Abstract
A method and system for packet based data communication between a first unit (1) and a second unit (3), wherein said first unit (1) communicate via an intermediate unit (2), each unit being identified by at least one address. The method comprises the steps of retrieving, at said first unit (1), from said intermediate unit (2) and address of said at least one address identifying said intermediate unit. The retrieved address is used as source address when forming a first data packet in said first unit (1). The data packet is tunneled from said first unit (1) to said intermediate unit (2) and then sent from said intermediate unit to said second unit.

French Abstract
L'invention concerne un procede et un systeme de transmission de donnees en paquets entre une premiere unite (1) et une seconde unite (3), ladite premiere unite (1) communiquant via une unite intermediaire (2), et chaque unite etant identifiee a l'aide d'au moins une adresse. Ledit procede consiste a extraire une adresse de l'adresse identifiant l'unite intermediaire, a partir de ladite unite intermediaire (2), au niveau de la premiere unite (1). L'adresse extraite est une adresse source

permettant la formation d'un premier paquet de donnees dans la premiere unite (1). Ledit paquet de donnees est soumis a un effet de tunnel de la premiere unite (1) vers l'unite intermediaire (2), puis envoye de ladite unite interme diaire vers la seconde unite.

Legal Status (Type, Date, Text)
Publication 20020516 A1 With international search report.
Examination 20021219 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... most
commonly used method to implement IPSec.

There are several problems with using solutions with **authentication** , encryption and/or data integrity **checks** implemented between the network layer, i.e. a TCP/IP stack, and the data link and physical layers. **IPSec** places severe constraints on the possibilities of changing data as it is passed over the network. This makes it impossible to change **IP** packet **headers** while in transit.

There are a number of situations when IP packets need to be...

26/5,K/17 (Item 15 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00895811 **Image available**
GROUP PACKET ENCAPSULATION AND COMPRESSION SYSTEM AND METHOD
ENCAPSULATION DE PAQUETS GROUPES ET SYSTEME ET PROCEDE DE COMPRESSION
Patent Applicant/Assignee:
PROVISIONPOINT COMMUNICATIONS LLC, 101 Brantwood Road, Arlingotn, MA 02476, US, US (Residence), US (Nationality)
Inventor(s):
HUANG Zezhen, 5 Beaver Road, Canotn, MA 02021, US,
Legal Representative:
MELLO David M (agent), McDermott, Will & Emery, 28 State Street, Boston, MA 02109, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200229991 A1 20020411 (WO 0229991)
Application: WO 2001US31086 20011004 (PCT/WO US0131086)
Priority Application: US 2000238213 20001005; US 2000238266 20001005; US 2000238138 20001005; US 2000241055 20001017; US 2001789852 20010221
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04B-001/66
International Patent Class: **H04L-009/00**

Publication Language: English
Filing Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 11269

English Abstract
  A group packet encapsulation and optionally compression system (Fig. 5A) and method (Fig. 5B), including an encapsulation protocol increases packet transmission performance between two gateways or host computers (602,604) by reducing data-link layer framing overhead, reducing packet routing overhead in gateways (602,604), compressing packet headers (558) in the encapsulation packet, and increasing loss-less data compression ratio beyond that otherwise achievable in typical systems. Packets queued at a node (500) configured in accordance with the present invention are classified, grouped (554), and encapsulated (556) into a single packet as a function of having another such configured node in their path. The nodes (500) exchange encapsulation packets, even though the packets within the encapsulation packet may ultimately have different destinations. Compression within an encapsulation packet may be performed on headers, payloads, or both.

French Abstract
  La presente invention concerne l'encapsulation de paquets groupes et eventuellement un systeme (fig. 5A) et un procede (fig. 5B) de compression. Dans ce procede, un protocole d'encapsulation ameliore les performances de transmission des paquets entre deux tetes de lignes ou deux ordinateurs hotes (602, 604) en reduisant les frais de structure de trame de la couche de liaison de donnees, en reduisant les frais d'acheminement des paquets dans les tetes de ligne (602, 604), en compressant les en-tetes (558) des paquets dans les paquets d'encapsulation, et en augmentant le taux de compression de donnees sans perte au dela des taux realisables par les systemes habituels. Les paquets en file d'attente dans un noeud (500) agence selon l'invention sont classifies, groupes (554) et encapsules (556) en un seul paquet en fonction de la presence d'un autre noeud ainsi agence dans leur cheminement. Ces noeuds (500) echangent des paquets d'encapsulation, meme si les paquets presents dans le paquet d'encapsulation peut avoir au final deux destinations differentes. On peut realiser la compression des en-tetes, des charges utiles ou de ces deux elements dans un paquet d'encapsulation.

Legal Status (Type, Date, Text)
Publication 20020411 A1 With international search report.

International Patent Class: **H04L-009/00**
Fulltext Availability:
  Detailed Description

Detailed Description
... address 768 of the IP packet-1 722 header may also be saved in the **encapsulation** payload 794 such that the IP packet- 1 722 header can be reconstructed by Node-Y 604. The GIEC **IP header** 762 also replaces other fields such as **checksum** , total length, and protocol ID in the IP packet-1 722 header. The protocol BD...

26/5,K/18 (Item 16 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00887138 **Image available**

MONITORING NETWORK TRAFFIC DENIAL OF SERVICE ATTACKS

SURVEILLANCE D'ATTAQUES DE TRAFIC DE RESEAU PAR REFUS DE SERVICE

Patent Applicant/Assignee:
MAZU NETWORKS INC, 6th floor, 125 Cambridge Park Drive, Cambridge, MA 02140, US, US (Residence), US (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:
POLETTO Massimiliano Antonio, 474 Broadway 6, Cambridge, MA 02138, US, US (Residence), IT (Nationality), (Designated only for: US)
KOHLER Edward W Jr, 805 57th Street, Oakland, CA 94608, US, US (Residence), US (Nationality), (Designated only for: US)

Legal Representative:
MALONEY Denis G (agent), Fish & Richardson, P.C., 225 Franklin Street, Boston, MA 02110-2804, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200221302 A1 20020314 (WO 0221302)
Application: WO 2001US27402 20010904 (PCT/WO US0127402)
Priority Application: US 2000230759 20000907; US 2001931558 20010816

Parent Application/Grant:
Related by Continuation to: US 2000230759 20000907 (CON); US 2001931558 20010816 (CON)

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Main International Patent Class: **G06F-015/76**
International Patent Class: G06F-011/30
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12856

English Abstract

A system architecture (10) for thwarting denial of service attacks on a victim data center (20) is described. The system includes a first plurality of monitors (26, 28) that monitor network traffic flow. The system includes a central controller (24) that receives data from monitors (26, 28), over a hardened, redundant network (30). The central controller (24) analyzes network traffic statistics to identify malicious network traffic. A gateway (26) is disposed to protect the victim site.

French Abstract

Cette invention concerne une architecture de systeme (10) permettant de contrecarrer des attaques par refus de service contre un centre de donnees (20). Le systeme comprend une premiere pluralite de moniteurs (26, 28) qui surveillent l'ecoulement du trafic au sein du reseau. Le systeme comprend une unite de commande centrale (24) qui recoit des donnees des moniteurs (26, 28) via un reseau redondant renforce (30). L'unite de commande centrale (24) analyse les statistiques relatives au trafic du reseau dans le but d'identifier un trafic malveillant sur le reseau. On trouve une passerelle (26) qui est concue pour proteger le site agresse.

Legal Status (Type, Date, Text)
Publication 20020314 A1 With international search report.
Publication 20020314 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20021121 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **G06F-015/76**
Fulltext Availability:
Detailed Description

Detailed Description
... send RST packets to B later if no ACK was received from A.

Expects IP **encapsulated** TCP packets, each with its **ip header** marked (MarkIPHeader(n) or CheckIPHeader(n)).

Aside from responding to SYN ACK packets from B, TCPSYN Proxy also **examines** SYN packets from A. When a SYN packet from A is received, if there are...

26/5,K/19 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00887133 **Image available**
ARCHITECTURE TO THWART DENIAL OF SERVICE ATTACKS
SURVEILLANCE D'ATTAQUES DE TRAFIC DE RESEAU PAR REFUS DE SERVICE
Patent Applicant/Assignee:
MAZU NETWORKS INC, 6th floor, 125 Cambridge Park Drive, Cambridge, MA 02140, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
KAASHOEK Marinus Frans, 2 Patriots Drive, Lexington, MA 02173, US, US (Residence), NL (Nationality), (Designated only for: US)
KOHLER Edward W Jr, 805 57th Street, Oakland, CA 94608, US, US (Residence), US (Nationality), (Designated only for: US)
POLETTO Massimiliano Antonio, 474 Broadway 6, Cambridge, MA 02138, US, US (Residence), IT (Nationality), (Designated only for: US)
Legal Representative:
MALONEY Denis G (agent), Fish & Richardson P.C., 225 Franklin Street, Boston, MA 02110-2804, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200221297 A1 20020314 (WO 0221297)
Application: WO 2001US27395 20010904 (PCT/WO US0127395)
Priority Application: US 2000230759 20000907; US 2001931561 20010816
Parent Application/Grant:
Related by Continuation to: US 2000230759 20000907 (CON); US 2001931561 20010816 (CON)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G06F-015/16**

International Patent Class: G06F-013/36; G07C-009/00; **H04L-009/00** ;
H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12746

English Abstract
A system architecture (10) for thwarting denial of service attacks on a victim data center is described. The system (10) includes a first plurality of monitors (28) that monitor network traffic flow through the network (14). The first plurality of monitors (28) is disposed at a second plurality of points in the network (14). The system (10) includes a central controller (24) that receives data from the plurality of monitors (18), over a hardened, redundant network (30). The central controller (24) analyzes network statistics to identify malicious network traffic. In some embodiments of the system, a gateway device (26) is disposed to pass network packets between the network (14) and the victim site (12). The gateway (26) is disposed to protect the victim site (12), and is coupled to the control center (24) by the redundant hardened network (30).

French Abstract
Cette invention concerne une architecture de systeme (10) permettant de contrecarrer des attaques par refus de service contre un centre de donnees. Le systeme (10) comprend une premiere pluralite de moniteurs (28) qui surveillent l'ecoulement du trafic au sein du reseau (14) . Cette premiere pluralite de moniteurs (28) est disposee au niveau d'une seconde pluralite de points dans le reseau (14). Le systeme (10) comprend une unite de commande centrale (24) qui recoit des donnees de la pluralite de moniteurs (18) via un reseau redondant renforce (30). L'unite de commande centrale (24) analyse les statistiques relatives au trafic du reseau dans le but d'identifier un trafic malveillant sur le reseau. Selon certains modes de realisation du systeme, un dispositif passerelle (26) est implante pour faire passer des paquets entre le reseau (14) et le site agresse (12). Cette passerelle (26) est concue pour proteger le site agresse (12) et est reliee au centre de commande (24) par le reseau redondant renforce (30).

Legal Status (Type, Date, Text)
Publication 20020314 A1 With international search report.
Publication 20020314 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20020912 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **G06F-015/16**
...International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description
Detailed Description
... send RST packets to B later if no ACK was received from A.

Expects IP **encapsulated** TCP packets, each with its **ip header** marked (MarkIPHeader(n) or CheckIPHeader(n)).

Aside from responding to SYN ACK packets from B, TCPSYN

Proxy also **examines** SYN packets from A. When a SYN packet from A is received, if there are...

26/5,K/20 (Item 18 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00887132 **Image available**
STATISTICS COLLECTION FOR NETWORK TRAFFIC
COLLECTE DE STATISTIQUES POUR TRAFIC DE RESEAU
Patent Applicant/Assignee:
MAZU NETWORKS INC, 6th Floor, 125 Cambridge Park Drive, Cambridge, MA 02140, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
GIL Thomer Michael, Sarphatistraat 590a, NL-1018 AV Amsterdam, NL, NL (Residence), NL (Nationality), (Designated only for: US)
POLETTO Massimiliano Antonio, 474 Broadway 6, Cambridge, MA 02138, US, US (Residence), IT (Nationality), (Designated only for: US)
KOHLER Edward W Jr, 805 57th Street, Oakland, CA 94608, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
MALONEY Denis G (agent), Fish & Richardson, P.C., 225 Franklin Street, Boston, MA 02110-2804, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200221296 A1 20020314 (WO 0221296)
Application: WO 2001US27394 20010904 (PCT/WO US0127394)
Priority Application: US 2000230759 20000907; US 2001931223 20010816
Parent Application/Grant:
Related by Continuation to: US 2000230759 20000907 (CON); US 2001931223 20010816 (CON)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G06F-015/16**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 13931

English Abstract
A system architecture for thwarting denial of service attacks on a victim data center (20). The system includes a first plurality of monitors (33) that monitor network traffic flow through the network (30). The first plurality of monitors (33) is disposed at a second plurality of points (28) in the network (30). The system includes a central controller (27) that receives data from the plurality of monitors (33) over a network (30). The central controller (27) analyzes network traffic statistics (35) to identify malicious network traffic.

French Abstract
Cette invention concerne une architecture de systeme permettant de contrecarrer des attaques par refus de service contre un centre de

donnees (20). Le systeme comprend une premiere pluralite de moniteurs (33) qui surveillent l'ecoulement du trafic au sein du reseau. Cette premiere pluralite de moniteurs (33) est disposee au niveau d'une seconde pluralite de points (28) dans le reseau. Le systeme comprend une unite de commande centrale (27) qui recoit des donnees de la pluralite de moniteurs (33) via un reseau (30). L'unite de commande centrale (27) analyse les statistiques (35) relatives au trafic du reseau dans le but d'identifier un trafic malveillant sur le reseau.

Legal Status (Type, Date, Text)
Publication 20020314 A1 With international search report.
Publication 20020314 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20020906 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **G06F-015/16**
Fulltext Availability:
Detailed Description

Detailed Description
... send RST packets to B later if no ACK was received from A.

Expects IP **encapsulated** TCP packets, each with its **ip header** marked (MarkIPHeader(n) or CheckIPHeader(n)).

Aside from responding to SYN ACK packets from B, TCPSYN Proxy also **examines** SYN packets from A. When a SYN packet from A is received, if there are...

26/5,K/21 (Item 19 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00887118 **Image available**
THWARTING SOURCE ADDRESS SPOOFING-BASED DENIAL OF SERVICE ATTACKS
PROTECTION CONTRE LES ATTAQUES PAR INTERRUPTION DE SERVICE FONDEES SUR LA MYSTIFICATION D'ADRESSE SOURCE
Patent Applicant/Assignee:
MAZU NETWORKS INC, 6th floor, 125 Cambridge Park Drive, Cambridge, MA 02140, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
KOHLER Edward W Jr, 805 57th Street, Oakland, CA 94608, US, US (Residence), US (Nationality), (Designated only for: US)
POLETTO Massimiliano Antonia, 474 Broadway 6, Cambridge, MA 02138, US, US (Residence), IT (Nationality), (Designated only for: US)
Legal Representative:
MALONEY Denis G (agent), Fish & Richardson, P.C., 225 Franklin Street, Boston, MA 02110-2804, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200221279 A1 20020314 (WO 0221279)
Application: WO 2001US27396 20010904 (PCT/WO US0127396)
Priority Application: US 2000230759 20000907; US 2001931487 20010816
Parent Application/Grant:
Related by Continuation to: US 2000230759 20000907 (CON); US 2001931487 20010816 (CON)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ

DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ
LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG
SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-011/30
International Patent Class: G06F-012/14; **G06F-015/16 ; G06F-015/173**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 13004

English Abstract
A system architecture for thwarting denial of service attacks on a victim data center is described. The system includes a first plurality of monitors that monitor network traffic flow through the network. The first plurality of monitors (28) is disposed at a second plurality of points in the network. The system includes a central controller (24) that receives data from the plurality of monitors (28), over a hardened, redundant network (30). The central controller (24) analyzes network traffic statistics to identify malicious network traffic. In some embodiments of the system, a gateway device (26) is disposed to pass network packets between the network (14) and the victim site (12). The gateway (26) is disposed to protect the victim site (12), and is coupled to the control center (24) by the redundant hardened network (30).

French Abstract
La presente invention concerne une architecture de systeme destinee a dejouer les attaques par interruption de service lancees contre un centre de donnees victime. Ce systeme comprend une premiere pluralite de demons qui surveillent un flux de trafic de reseau a travers ce reseau. Cette premiere pluralite de demons (28) est placee au niveau d'une seconde pluralite de points de ce reseau. Ce systeme comprend un controleur (24) central qui recoit des donnees de la pluralite de demons (28), via un reseau (30) redondant renforce. Ce controleur (24) central analyse les statistiques de trafic du reseau de facon a reperer un trafic de reseau malveillant. Dans certains modes de realisation de l'invention, un dispositif de passerelle (26) est place de facon a faire passer les paquets de reseau entre ce reseau (14) et le site victime (12). Cette passerelle (26) est placee de facon a proteger le site victime (12), et elle est couplee au centre (24) de commande par le reseau (30) redondant renforce.

Legal Status (Type, Date, Text)
Publication 20020314 A1 With international search report.
Publication 20020314 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20021017 Request for preliminary examination prior to end of 19th month from priority date

...International Patent Class: **G06F-015/16** ...

... **G06F-015/173**
Fulltext Availability:
Claims

Claim
... send RST packets to B later if no ACK was
received from A.
Expects IP **encapsulated** TCP packets, each with its **ip header** marked (MarkIPHeader(n) or CheckIPHeader(n)). Aside from
responding to SYN ACK packets from B, TCPSYN
Proxy also **examines** SYN packets from A. When a SYN packet
from A is received, if there are...

26/5,K/22 (Item 20 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00887117 **Image available**
COORDINATED THWARTING OF DENIAL OF SERVICE ATTACKS
PROCEDE PERMETTANT DE CONTRECARRER DE MANIERE COORDONNEE DES ATTAQUES PAR REFUS DE SERVICE
Patent Applicant/Assignee:
MAZU NETWORKS INC, 6th floor, 125 Cambridge Park Drive, Cambridge, MA 02140, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
KAASHOEK Marinus Frans, 2 Patriots Drive, Lexington, MA 02173, US, US (Residence), NL (Nationality), (Designated only for: US)
KOHLER Edward W Jr, 805 57th Street, Oakland, CA 94608, US, US (Residence), US (Nationality), (Designated only for: US)
POLETTO Massimiliano Antonio, 474 Broadway 6, Cambridge, MA 02138, US, US (Residence), IT (Nationality), (Designated only for: US)
MORRIS Robert T, *, (Designated only for: US)
Legal Representative:
MALONEY Denis G (agent), Fish & Richardson P.C., 225 Franklin Street, Boston, MA 02110-2804, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200221278 A1 20020314 (WO 0221278)
Application: WO 2001US27244 20010904 (PCT/WO US0127244)
Priority Application: US 2000230759 20000907; US 2001931291 20010816
Parent Application/Grant:
Related by Continuation to: US 2001931291 20010816 (CON); US 2000230759 20000907 (CON)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-011/30
International Patent Class: **G06F-015/16 ; G06F-015/173**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12676
English Abstract
A system architecture for thwarting denial of service attacks (10) on a victim data center (12) is described. The victim (12) is coupled to the Internet (14) or other network. An attacker via computer system (16) that is connected to the Internet e.g., via an Internet (14) Service Provider

(18), infiltrates one or a plurality of computers at various other sites or data centers (20a-20c). The arrangement (10) to protect the victim control center (24) that communicates with and controls gateways (26) and data collectors (28) disposed in the network (14). The control center (24) is couped to the gateways (26) and data collectors (28) by a hardened, redundant network (30). The gateways (26) and data collectors (28) constantly analize traffic, looking for congestion or traffic levels that indicate an attack on the Internet or network (14).

French Abstract

Cette invention a trait a une architecture de systeme permettant de contrecarrer des attaques par refus de service (10) dirigees contre un centre de donnees victime (12). La victime (12) est connectee a l'Internet (14) ou a un autre reseau. Un agresseur infiltre, par le biais d'un systeme informatique (16) connecte a l'Internet, par exemple par le canal d'un prestataire de services de l'Internet (18), un ou plusieurs ordinateurs sur divers autres sites ou centres de donnees (20a 20c). Le dispositif (10) selon l'invention, destine a proteger la victime, comporte un centre de commande (24) qui communique avec des passerelles (26) et des collecteurs de donnees (28) se trouvant dans le reseau (14) et les commande. Le centre de commande (24) est connecte aux passerelles (26) et aux collecteurs de donnees par un reseau fortifie redondant (30). Les passerelles (26) et les collecteurs de donnees (28) analysent sans interruption le trafic afin de surveiller la survenue d'une congestion ou de niveaux de trafic representatifs d'une attaque sur l'Internet ou le reseau (14).

Legal Status (Type, Date, Text)
Publication 20020314 A1 With international search report.
Examination 20021107 Request for preliminary examination prior to end of 19th month from priority date

International Patent Class: **G06F-015/16** ...

... **G06F-015/173**
Fulltext Availability:
Detailed Description

Detailed Description
... send RST packets to B later if no ACK was received from A.

Expects IP **encapsulated** TCP packets, each with its **ip header** marked (MarkIPHeader(n) or CheckIPHeader(n)).

Aside from responding to SYN ACK packets from B, TCPSYN Proxy also **examines** SYN packets from A. When a SYN packet from A is received, if there are...

26/5,K/24 (Item 22 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00865693 **Image available**
METHOD AND APPARATUS FOR INTERFACING A NETWORK TO AN EXTERNAL ELEMENT
PROCEDE ET APPAREIL INTERFACANT UN RESEAU ET UN ELEMENT EXTERNE
Patent Applicant/Assignee:
MOTOROLA INC, 1303 East Algonquin Road, Schaumburg, IL 60196, US, US (Residence), US (Nationality)
Inventor(s):

BANKS Robert, 4921 Lichfield Drive, Barrington, IL 60010, US,
JONES Wesley Stuart, 643 East Monterey Road, Palatine, IL 60067, US,
MALCOLM Richard, 625 Paxton Place, Carol Stream, IL 60188, US,
Legal Representative:
MAY Steven A (et al) (agent), Motorola, Inc., Intellectual Property Dept., 1303 East Algonquin Road, Schaumburg, IL 60196, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200199334 A1 20011227 (WO 0199334)
Application: WO 2001US14030 20010501 (PCT/WO US0114030)
Priority Application: US 2000597315 20000620
Designated States: KR
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
Main International Patent Class: **H04L-009/00**
International Patent Class: H04K-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4016

English Abstract
A services delivery element (26) forms an interface between an external element (such as an external end user's network feature server) and a communication network including both a core network (10) and an access network (12). The services delivery element (26) provides access to the core network (10) and access networks (12) to which the external element is interfaced.

French Abstract
Un element de distribution de services (26) forme une interface entre un element externe (tel qu'un serveur de caracteristiques de reseau d'un utilisateur final externe) et un reseau de communication comportant un reseau central (10) et un reseau d'acces (12). L'element de distribution de services (26) fournit un acces au reseau central (10) et aux reseaux d'acces (12) auxquels l'element externe est interface.

Legal Status (Type, Date, Text)
Publication 20011227 A1 With international search report.
Examination 20020530 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... this mode of operation, both the external API 22 and the internal API 18 will **authenticate** and encrypt the entire IP source packet and **wrap** a
new **IP** **header** around them. ESP in **tunnel** mode encrypts and optionally
authenticates the entire inner IP packet, including the inner **IP** **header** . AH in **tunnel** mode **authenticates** the entire inner IP packet and selected portions of the outer **IP** **header** .

Since, as described, the services delivery element 26/ external API 22 **IPSec** transmissions will be in **tunnel** mode, all of the hosts inside the core network 1 0 will
communicate with the...

26/5,K/25 (Item 23 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00833723 **Image available**

NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA NETWORKS USING LOCAL IP ADDRESSES AND NON-TRANSLATABLE PORT ADDRESSES

PASSERELLE DE TRADUCTION D'ADRESSES RESEAU POUR RESEAUX LOCAUX D'ENTREPRISE UTILISANT DES ADRESSES IP LOCALES ET DES ADRESSES DE PORT NON TRADUISIBLES

Patent Applicant/Assignee:
NEXLAND INC, North Tower, 2nd Floor, 1101 Brickell Avenue, Miami, FL 33131, US, US (Residence), US (Nationality)
Inventor(s):
SULTAN Israel Daniel, 9, rue Caillaux, F-75013 Paris, FR,
Legal Representative:
CESARANO Michael C (agent), Akerman, Senterfitt & Eidson, P.A., Suntrust International Center, 28th Floor, 1 S.E. 3rd Avenue, Miami, FL 33131-1714, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200167258 A1 20010913 (WO 0167258)
Application: WO 2001US6257 20010227 (PCT/WO US0106257)
Priority Application: US 2000518399 20000303
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-013/00
International Patent Class: **G06F-015/16** ; **H04L-009/00** ; H04L-013/10
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10804

English Abstract
A network address translation gateway (20) provides normal network translation for IP datagrams traveling from a local area network (10) using local IP addresses to an external network (30), but suspends source service address (port) translation when the port is reserved for a specific protocol, such as the ISAKMP "handshaking" protocol that is part of the IPSec protocol model (FIGs. 2 and 3). ISAKMP exchanges require both source and target computers to use the same service address (port). By providing a network interface that does not translate the source service address (port), this gateway enables the initiation and maintenance of secure, encrypted transmissions using IPSec protocol between a local area network using local IP addresses and servers on the internet.

French Abstract
Une passerelle de traduction d'adresses reseau (20) assure la traduction reseau normale de datagrammes IP circulant entre un reseau local d'entreprise (10) utilisant des adresses IP locales et un reseau externe (30), mais suspend la traduction des adresses de service sources (port) lorsque le port est reserve a un protocole specifique, tel que le

protocole de transfert ISAKMP faisant partie du modele de protocole IPSec (Fig. 2 et 3). Pour les echanges ISAKMP, les ordinateurs sources et cibles doivent utiliser la meme adresse de service (port). Grace a une interface de reseau qui ne traduit pas l'adresse de service source (port), ladite passerelle permet le lancement et le maintien d'emissions chiffrees sures, a l'aide du protocole IPSec, entre un reseau local d'entreprise utilisant des adresses IP locales et des serveurs sur Internet.

Legal Status (Type, Date, Text)
Publication 20010913 A1 With international search report.
Examination 20011213 Request for preliminary examination prior to end of 19th month from priority date

International Patent Class: **G06F-015/16** ...

... **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... for the
4
datagram. Further information regarding these protocols may be found in RFC1 826, " **IP Authentication Header** ," by R.Atkinson (August 1995), and RFC2406, "IP **Encapsulating** Security Payload (ESP)," S. Kent and R. Atkinson (November 1998).

ISAKIVIP/Oakley (Internet Security Association...

26/5,K/26 (Item 24 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00821330 **Image available**
METHOD, SYSTEM FOR TRANSMITTING DATA FROM A TRANSMITTER TO A RECEIVER AND TRANSMITTER OR RECEIVER
PROCEDE ET SYSTEME DE TRANSMISSION DE DONNEES D'UN EMETTEUR VERS UN RECEPTEUR ET EMETTEUR OU RECEPTEUR A CET EFFET
VERFAHREN, SYSTEM ZUR UBERMITTLUNG VON DATEN VON EINEM SENDER ZU EINEM EMPFANGER UND SENDER BZW. EMPFANGER HIERZU
Patent Applicant/Assignee:
SIEMENS AKTIENGESELLSCHAFT, Wittelsbacherplatz 2, 80333 Munchen, DE, DE (Residence), DE (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
EUCHNER Martin, Lorenzstrasse 2, 81737 Munchen, DE, DE (Residence), DE (Nationality), (Designated only for: US)
Legal Representative:
SIEMENS AKTIENGESELLSCHAFT (commercial rep.), Postfach 22 16 34, 80506 Munchen, DE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200154371 A2-A3 20010726 (WO 0154371)
Application: WO 2001DE21 20010105 (PCT/WO DE0100021)
Priority Application: DE 10001855 20000118
Designated States: CA JP US
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-029/06
Publication Language: German
Filing Language: German
Fulltext Availability:

Detailed Description
Claims
Fulltext Word Count: 3672

English Abstract
A method and system for transmitting data from a transmitter to a receiver, wherein data from a transmitter is extended to include authentication data on the application level by means an application protocol. Said authentication data is used by the receiver to determine whether the transmitter is known by the receiver. If the transmitter is known by the receiver, the data is accepted. If not, the data is rejected.

French Abstract
L'invention concerne un procede de transmission de donnees d'un emetteur vers un recepteur, selon lequel l'emetteur complete les donnees avec des donnees d'authentification sur la couche d'application au moyen d'un protocole d'application. A l'aide des donnees d'authentification, le recepteur determine s'il connait l'emetteur. Si le recepteur connait l'emetteur, les donnees sont admises, dans le cas contraire, les donnees sont rejetees.

German Abstract
Es wird ein Verfahren zur Ubermittlung von Daten von einem Sender zu einem Empfanger angegeben, bei dem von dem Sender die Daten mittels eines Anwendungsprotokolls auf der Anwendungsschicht um Authentisierungsdaten erweitert werden. Anhand der Authentisierungsdaten wird von dem Empfanger ermittelt, ob er den Sender kennt. Falls der Empfanger den Sender kennt, werden die Daten entgegengenommen, ansonsten werden die Daten verworfen.

Legal Status (Type, Date, Text)
Publication 20010726 A2 Without international search report and to be republished upon receipt of that report.
Examination 20011108 Request for preliminary examination prior to end of 19th month from priority date
Search Rpt 20020328 Late publication of international search report
Republication 20020328 A3 With international search report.

Fulltext Availability:
Claims

Claim
... Internet Key Exchange (IKE), D. Harkins, D. Carrel, ; Internet Engineering Task Force, 1998.
[51 [RFC24021 **IP Authentication Header** , S. Kent, R. Atkinson; Internet Engineering Task Force, 1998. [6] [RFC24061 IP **Encapsulating** Security Payload (ESP), S. Kent, R. Atkinson; Internet Engineering Task Force, 1998.
Patentanspruche

1 Verfahren...

26/5,K/27 (Item 25 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00785490 **Image available**
INTERNET PROTOCOL MOBILITY ARCHITECTURE FRAMEWORK
CADRE D'ARCHITECTURE DE MOBILITE PAR PROTOCOLE INTERNET
Patent Applicant/Assignee:

NORTEL NETWORKS LIMITED, World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4, CA, CA (Residence), CA (Nationality)
Inventor(s):
AKHTAR Haseeb, 3102 Pamela Place, Garland, TX 75044, US,
QADDOURA Emad A, 1320 Wateredge Drive, Plano, TX 75093, US,
BECKER Carey B, 1529 Faringdon Drive, Plano, TX 75075, US,
PATIL Basavaraj B, 7616 Capella Court, Plano, TX 75025, US,
BARNES March H, 3820 Hidden Trail, Flower Mound, TX 75028, US,
WURCH Donald L, 3607 Highpoint Drive, Rockwall, TX 75078, US,
COFFIN Russell C, 5608 Crowndale Drive, Plano, TX 75093-8500, US,
ZHU Zemin, 3808 Neiman Road, Plano, TX 75025, US,
TUMMALA Rambabu, 4324 Giovanni, Plano, TX 75024, US,
NARAYANAN Raja, 1100 Meredith Lane #728, Plano, TX 75093, US,
KHALIL Mohamed, 118 Briaroaks Street, Murphy, TX 75095, US,
LE Liem Q, 1605 Meadowgate Drive, Richardson, TX 75081, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200119050 A2-A3 20010315 (WO 0119050)
Application: WO 2000IB1553 20000908 (PCT/WO IB0001553)
Priority Application: US 99152916 19990908; US 99156669 19990929; US 99157289 19991001; US 99157449 19991004; US 2000192411 20000327; US 2000657516 20000907
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
International Patent Class: H04Q-007/24
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 85222
English Abstract
A communications architecture for enabling IP-based mobile communications includes a Local Service Function (LSF) component configured to serve as an IP-based serving area network for a set of x-Access Networks, and a Network Service Function (NSF) component configured to serve as an IP-based home network by managing a MN's subscription and associated profile so that the MN is authorized to use the resources of the LSF. An x-Access Network (xAN) is interconnected to the LSF and NSF for providing heterogeneous Layer (2) access for MNs irrespective of access technology.

French Abstract
La presente invention concerne une architecture de communications permettant d'etablir des communications mobiles par protocole IP, comportant un composant a fonction de services locaux (LSF) concu pour agir comme un reseau a zone de desserte IP pour un ensemble de reseaux d'acces x, et un composant a fonction de services reseau (NSF) concu pour agir comme un reseau local IP en gerant un abonnement a un noeud mobile (MN) et son profil associe de sorte que le MN soit autorise a utiliser les ressources de la fonction LSF. Un reseau d'acces x (xAN) est interconnecte aux LSF et NSF pour fournir a une couche heterogene (2) l'acces aux MN quelle que soit la technologie d'acces.
Legal Status (Type, Date, Text)
Publication 20010315 A2 Without international search report and to be

republished upon receipt of that report.
Examination 20010719 Request for preliminary examination prior to end of 19th month from priority date
Search Rpt 20011122 Late publication of international search report
Republication 20011122 A3 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... 426 'may cache the
previous IP address, the CN applications will not be able
to **communicate** with the user's application 414 or 424.

This may be overcome by setting the **Time** To **Live** (**TTL**)
contained within the record of the home DDNS 456 to zero,
indicating that the CN...

26/5,K/28 (Item 26 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00771639 **Image available**
TRANSMISSION OF COMPRESSED INFORMATION WITH REAL TIME REQUIREMENT IN A PACKET ORIENTED INFORMATION NETWORK
TRANSMISSION D'INFORMATIONS COMPRIMEES AVEC CONTRAINTE TEMPS REEL DANS UN RESEAU D'INFORMATION ORIENTE PAQUETS
Patent Applicant/Assignee:
TELEFONAKTIEBOLAGET LM ERICSSON (publ), S-126 25 Stockholm, SE, SE (Residence), SE (Nationality)
Inventor(s):
GALYAS Johan Karoly Peter, Slottsvagen 31, S-183 52 Taby, SE
Legal Representative:
NORIN Klas, Ericsson Radio Systems AB, Common Patent Department, S-164 80 Stockholm, SE
Patent and Priority Information (Country, Number, Date):
Patent: WO 200105172 A1 20010118 (WO 0105172)
Application: WO 2000SE1356 20000627 (PCT/WO SE0001356)
Priority Application: SE 992655 19990709
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04Q-007/22
International Patent Class: H03M-013/09
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9022

English Abstract
The present invention relates to packet-distributed data transmission of compressed data. According to the invention, parity bits are supplied to the compressed data. The parity bits are used in the entire transmission

chain between an encoder having compressed the data, and a decoder which decompresses it. According to one embodiment, the data is speech and the packet-distributed network is a mobile radio network with packet-distribution in included links. However, sending in the radio link of the compressed speech is circuit switched.

French Abstract
Cette invention se rapporte a la transmission de donnees comprimees avec distribution par paquets. Selon cette invention, des bits de parite sont appliques aux donnees comprimees. Ces bits de parite sont utilises dans toute la chaine de transmission entre un codeur ayant comprime les donnees et un decodeur qui les decomprime. Selon un mode de realisation, les donnees sont des signaux vocaux et le reseau de distribution par paquets est un reseau de radiocommunication mobile avec distribution des paquets dans des liens inclus, l'emission dans le lien de radiocommunication des signaux vocaux comprimes etant toutefois commutee par circuit.

Legal Status (Type, Date, Text)
Publication 20010118 A1 With international search report.
Publication 20010118 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.
Examination 20010405 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims

Claim
... sending gateway in the speech encoder unit I 1. The UDP header also contains a **check** sum, i.e. parity bits, intended to be used for discovering any case of data being distorted during the transmission. The IP layer **wraps** the UDP message in an IT packet. The IP packet comprises, apart from the UDP message, an **IP header** with an IP address to the base station BTS in question. By means of the...

26/5,K/29 (Item 27 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00764560 **Image available**
A METHOD AND ARRANGEMENT FOR PROVIDING SECURITY THROUGH NETWORK ADDRESS TRANSLATIONS USING TUNNELING AND COMPENSATIONS
RECOURS A LA TUNNELISATION ET AUX CORRECTIONS POUR LA SECURISATION PAR TRADUCTIONS D'ADRESSES RESEAU, ET DISPOSITIF A CET EFFET
Patent Applicant/Assignee:
SSH COMMUNICATIONS SECURITY LTD, Tekniikantie 12, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
KIVINEN Tero, Magnus Enckellin kuja 9 K 19, FIN-02610 Espoo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
YLONEN Tatu, Taysikuu 10 C 88, FIN-02210 Espoo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
BERGGREN OY AB, P.O. Box 16, FIN-00101 Helsinki, FI
Patent and Priority Information (Country, Number, Date):
Patent: WO 200078008 A1 20001221 (WO 0078008)
Application: WO 2000FI537 20000615 (PCT/WO FI0000537)
Priority Application: US 99333829 19990615

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE
DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC
LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI
SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10534

English Abstract
This invention provides a method for providing network security services, such as those provided by the IPSEC protocol, through network address translation (NAT). The method is based on determining the transformations that occur on a packet and compensating for the transformations. Because only TCP and UDP protocols work through NATs, the IPSEC AH/ESP packets are encapsulated into UDP packets for transport. Special operations are performed to allow reliable communications in such environments.

French Abstract
L'invention concerne un procede permettant la realisation de services de securite de reseau, tels que ceux assures par le protocole IPsec, via la traduction des adresses reseau. Ledit procede repose sur la determination des transformations subies par un paquet et la correction de ces transformations. Du fait que seuls les protocoles TCP et UDP utilisent la traduction des adresses reseau, on encapsule les paquets AH/ESP d'IPsec en paquets UDP pour le transport. Des operations speciales permettent ensuite d'assurer des communications fiables dans de tels environnements.

Legal Status (Type, Date, Text)

Publication	20001221	A1 With international search report.
Publication	20001221	A1 Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.
Examination	20010222	Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims
Claim
... IP or Internet Protocol, which itself
has been specified in the RFC document number RFC791. **IPSEC** performs **authentication** and encryption on packet level by generating a new **IP header** , adding an **Authentication** Header (AH) or **Encapsulating** Security Payload (ESP) header in front of the packet. The original packet is cryptographically **authenticated** and optionally encrypted. The method used to **authenticate** and possibly encrypt a packet . identified by a security parameter index (SPI) value stored in...remote host, which were determined during the IKE negotiation. The receiver decapsulates packets from this **encapsulation** before doing AH or ESP processing. Decapsulation removes this header and updates the Protocol, Length, and **Checksum** fields of the **IP header** . No configuration data (port number etc.) is needed for this operation. The decapsulation should be...the Internet Protocol, RFC 2401, Internet Engineering Task Force, 1998. RFC2402

S. Kent, R. Atkinson: **IP Authentication Header** , RFC 2402, Internet Engineering Task Force, 1998.
RFC2406
S. Kent, R. Atkinson: IP **Encapsulating** Security Payload, RFC 2406, Internet Engineering Task Force, 1998.
RFC2407
D. Piper: The Internet IP...

26/5,K/30 (Item 28 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00742649 **Image available**
METHOD AND SYSTEM FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION WITH NETWORK SECURITY FEATURES
PROCEDE ET SYSTEME DESTINES A LA TRADUCTION REPARTIE D'ADRESSES RESEAU A L'AIDE DE DISPOSITIFS DE SECURITE DE RESEAU
Patent Applicant/Assignee:
3COM CORPORATION, 3800 Golf Road, Rolling Meadows, IL 60008, US, US (Residence), US (Nationality)
Inventor(s):
GRABELSKY David A, 3800 Lee Street, Skokie, IL 60076, US
BORELLA Michael S, 1208 Haverhill Circle, Naperville, IL 60563, US
SIDHU Ikhlaq S, 403 East River Grove Lane, Vernon Hills, IL 60061, US
NESSETT Danny M, 34810 Wabash River Place, Fremont, CA 94555, US
Legal Representative:
LESAVICH Stephen, McDonnell Boehnen Hulbert & Berghoff, 300 South Wacker Drive, Chicago, IL 60606, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200056034 A1 20000921 (WO 0056034)
Application: WO 2000US7057 20000315 (PCT/WO US0007057)
Priority Application: US 99270967 19990317
Designated States: CA DE GB JP
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-029/06
International Patent Class: H04L-029/12
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 24220

English Abstract
A method and system for distributed network address translation with security features. The method and system allow Internet Protocol security protocol ("IPsec") to be used with distributed network address translation. The distributed network address translation is accomplished with IPsec by mapping a local Internet Protocol ("IP") address of a given local network device and an IPsec Security Parameter Index ("SPI") associated with an inbound IPsec Security Association ("SA") that terminates at the local network device. A router allocates locally unique security values that are used as the IPsec SPIs. A router used for distributed network address translation is used as a local certificate authority that may vouch for identities of local network devices, allowing local network devices to bind a public key to a security name space that combines a global IP address for the router with a set of locally unique port numbers used for distributed network address translation. The router issues security certificates and may itself be authenticated by a higher certificate authority. Using a security

certificate, a local network device may initiate and be a termination point of an IPsec security association to virtually any other network device on an IP network like the Internet or an intranet. The method and system may also allow distributed network address translation with security features to be used with Mobile IP or other protocols in the Internet Protocol suite.

French Abstract
L'invention concerne un procede et un systeme destines a la traduction repartie d'adresses reseau a l'aide de dispositifs de securite. Ledit procede et ledit systeme permettent d'utiliser le critere de securite Internet Protocole ("IPsec") pour la traduction repartie d'adresses reseau. La traduction repartie d'adresses reseau est effectuee avec le protocole IPsec en etablissant, d'une part, une table de correspondances d'une adresse Internet (<= IP >=)d'un systeme reseau local et, d'autre part, un index des parametres de securite IPsec (<= SPI >=) combine a une association de securite IPsec (<= SA >=) qui s'arrete au systeme reseau local. Un routeur attribue localement des valeurs uniques de securite utilisees comme index des parametres de securite IPsec. Un routeur de traduction repartie d'adresses reseau est utilise comme organisme de certification local pouvant repondre des identites des systemes reseau locaux, autorisant lesdits systemes reseau locaux a associer une cle publique a un espace nom de securite, qui combine une adresse IP globale destinee au routeur et un ensemble de nombres de ports locaux uniques utilises pour la traduction repartie d'adresses reseau. Le routeur delivre des certificats de securite et peut lui meme etre authentifie par un organisme de certification superieur. S'il se sert d'un certificat de securite, un systeme reseau local peut demarrer ou etre le point final d'une association de securite IPsec avec pratiquement tout autre systeme reseau sur un reseau IP tel qu'Internet ou un reseau Intranet. Le procede et le systeme selon l'invention permettent egalement la traduction repartie d'adresses reseau a l'aide de dispositifs de securite faisant appel au Mobile IP ou a d'autres protocoles figurant dans la suite IP.

Legal Status (Type, Date, Text)
Publication 20000921 A1 With international search report.
Publication 20000921 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20001123 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... than an IP 48 address for an initiator's identity.

Certificates are issued with a " **Time** -to- **Live** " value, after which they expire and become invalid. The result of negotiation and **authentication** is a **secure connection**
260 (FIG. 18) for one unidirectional SA. A second SA for bi-directional communications may...

26/5,K/31 (Item 29 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00559417 **Image available**
LAYER TWO TUNNELING PROTOCOL (L2TP) MERGING AND MANAGEMENT

INTERCLASSEMENT ET GESTION DE PROTOCOLE TUNNEL A DEUX COUCHES (L2TP)

Patent Applicant/Assignee:
ASC - ADVANCED SWITCHING COMMUNICATIONS,
Inventor(s):
LOEHNDORF James R Jr,
NAUDUS Stanley T Jr,
MILLER D Richard Jr,
HSU Chang-Shan,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200022790 A1 20000420 (WO 0022790)
Application: WO 99US23217 19991006 (PCT/WO US9923217)
Priority Application: US 98103589 19981009; US 99251915 19990219
Designated States: AU BR CA CN JP KR MX SG ZA AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-012/66
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10304

English Abstract

A system is provided for creating a tunneling service from the use of a traditional tunneling protocol, such as layer two tunneling protocol (L2TP). In particular, the L2TP tunneling protocol, which is designed to go point-to-point between an L2TP Access Concentrator (LAC) (21, 22, 23) and an L2TP Network Server (LNS) (25, 26), is abstracted so that L2TP becomes an access protocol to the tunneling service. A new L2TP tunnel merger and management (LTM) service (20) is created which serves the tight configuration relationships between LAC (21, 22, 23) and LNSs (25, 26). Only a tight configuration between an LAC (21) and its LTM edge device (201) and between an LNS (251) and its LTM edge device (204) is required. An internal trunk protocol (INT protocol) carries needed information between the LTM edge devices to establish ingress/egress L2TP access calls inside of separate L2TP access tunnels on opposite LTM edge devices.

French Abstract

L'invention porte sur un systeme visant a creer un service tunnel a l'aide d'un protocole tunnel traditionnel tel qu'un protocole tunnel a deux couches (L2TP). Ce protocole tunnel L2TP, concu pour aller point a point entre un concentrateur d'acces L2TP (LAC) (21, 22, 23) et un serveur de reseau L2TP (LNS) (25, 26), est abrege de sorte que L2TP devienne un protocole d'acces au service tunnel. Un nouveau service (20) d'interclassement et de gestion tunnel L2TP est cree de facon a servir la relation de configuration etroite entre LAC (21, 22, 23) et LNS (25, 26). Seule une configuration etroite entre un LAC (21) et son dispositif (201) de bord d'interclassement et de gestion tunnel (LTM) et entre un LNS (251) et son dispositif (204) de bord LTM est necessaire. Un protocole de reseau interne (protocole INT) supporte les informations necessaires entre les dispositifs de bord LTM de facon a etablir des appels d'acces L2TP entree/sortie a l'interieur de tunnels d'acces L2TP separes sur des dispositifs de bord LTM opposes.

Fulltext Availability:
Detailed Description
Claims

Detailed Description

... block 63, the IP and UDP source and destination addresses are added to the IP **check** sum. In block 64, the new L2TP tunnel ID and call ID are

moved into the **L2TP** header. In block 65, the **L2TP** **tunnel** ID and call ID are added to the UDP **checksum** and, in block 66, the IP **hop** **count** is decremented. Finally, in block 67, the payload is forwarded to the LAC/LNS.

In...

Claim
... routing of L2TP access calls and associated data is based on information provided by an **L2TP** **tunnel** layer.

13 The system recited in claim 12, wherein the LTM service passes the Internet **Protocol** (**IP**) **header** and User Datagram **Protocol** (UDP) **header**
information and performs as needed updating of UDP and IP **check** sums.

14 The system recited in claim.3, wherein an LAC communicates a desired destination...of routing of L2TP` access calls and associated data based on information provided by an **L2TP** **tunnel** layer.

42 The method recited in claim 41, further comprising the step of passing the LTM service Internet **Protocol** (JP) **header** and User Datagram **Protocol** (UDP) **header** information with as needed processing of updating UDP and IP **check** sums.

43 The method recited in claim 32, further comprising the step of communicating by...

26/5,K/33 (Item 31 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00385992 **Image available**
KEY MANAGEMENT FOR NETWORK COMMUNICATION
GESTION DE CLEF POUR TRANSMISSION PAR RESEAU
Patent Applicant/Assignee:
RAPTOR SYSTEMS INC,
Inventor(s):
LEVESQUE Roger H,
KRAEMER Jeffrey A,
NADKARNI Ashok P,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9726735 A1 19970724
Application: WO 97US667 19970116 (PCT/WO US9700667)
Priority Application: US 96586231 19960116
Designated States: AU CA IL JP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-009/00**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 3624

English Abstract
The invention features a method for enabling computers (16, 18) to communicate using encrypted network packets. A configuration request is sent over a network (20, 21) from a first computer (16) to a second computer (18), and tunnel record information is sent over the network

(20, 21) from the second computer (18) to the first computer (16). The tunnel record information is encrypted in accordance with a temporary configuration password. The invention also features a method for updating a tunnel record. A connection request is sent from a first computer (16) to a second computer (18), and the first computer (16) is authorized. A tunnel record corresponding to the connection request with the first computer's network address is then updated.

French Abstract

L'invention porte sur un procede permettant a des ordinateurs (16, 18) de communiquer a l'aide de paquets codes de reseau. Un premier ordinateur (16) envoie, sur un reseau (20, 21), une demande de configuration a un second ordinateur (18) qui adresse, sur le reseau (20, 21), une information relative a un enregistrement de tunnel au premier (16). Cette information d'enregistrement de tunnel est codee en fonction d'un mot de passe provisoire de configuration. Elle porte egalement sur un procede de mise a jour d'enregistrement de tunnel. Un premier ordinateur (16) envoie une demande de connexion a un second ordinateur (18) et recoit une autorisation. Un enregistrement de tunnel correspondant a la demande de connexion avec l'adresse de reseau du premier ordinateur est alors mis a jour.

Main International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... 84,
After decryption, the security network driver issues (step 114, Fig. 7) a digital signature **check** call to **encapsulate** /decapsulate library 76, The swIPe **protocol header** includes a digital signature 86. The digital signature is a unique number calculated using the...

26/5,K/34 (Item 32 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00385991 **Image available**
TRANSFERRING ENCRYPTED PACKETS OVER A PUBLIC NETWORK
TRANSFERT DE PAQUETS CODES SUR UN RESEAU PUBLIC
Patent Applicant/Assignee:
RAPTOR SYSTEMS INC,
Inventor(s):
KIRBY Alan J,
KRAEMER Jeffrey A,
NADKARNI Ashok P,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9726734 A1 19970724
Application: WO 97US666 19970116 (PCT/WO US9700666)
Priority Application: US 96586230 19960116
Designated States: AU CA IL JP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-009/00**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4615

English Abstract
The invention features receiving encrypted network packets sent over a network (20) at a network interface computer (16) and passing the encrypted network packets to a computer (18) on an internal network. The invention further features receiving network packets sent over a network (20), determining which virtual tunnel (140, 142) each network packet was sent over, and routing each network packet to a destination computer in accordance with the determined virtual tunnel (140, 142).

French Abstract
L'invention porte sur la reception de paquets de reseau chiffres, envoyes sur un reseau (20), par un ordinateur interface de reseau (16) ainsi que sur l'envoi de paquets de reseau chiffres a un ordinateur (18) sur un reseau interne. L'invention porte, en outre, sur la reception de paquets de reseau envoyes sur un reseau (20), sur la determination du tunnel virtuel (140, 142) ayant servi a transmettre chaque paquet de reseau ainsi que sur l'acheminement de chaque paquet de reseau vers un ordinateur destinataire en fonction du tunnel virtuel determine (140, 142).

Main International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... 84.

After decryption, the security network driver issues (step 114, Fig* 7) a digital signature **check** call to **encapsulate** /decapsulate library 76. The swIPe **protocol header** includes a digital signature 86. The digital signature is a unique number calculated using the...

26/5,K/35 (Item 33 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00385988 **Image available**
DATA ENCRYPTION/DECRYPTION FOR NETWORK COMMUNICATION
CRYPTAGE/DECRYPTAGE DE DONNEES POUR COMMUNICATIONS SUR RESEAU
Patent Applicant/Assignee:
RAPTOR SYSTEMS INC,
Inventor(s):
LEVESQUE Roger H,
KIRBY Alan J,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9726731 A1 19970724
Application: WO 97US640 19970116 (PCT/WO US9700640)
Priority Application: US 96585765 19960116
Designated States: AU CA IL JP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-009/00**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4920
English Abstract
Security network driver software (72) is inserted between the network protocol TCP/IP and the corresponding network driver (40). Security

measures are performed upon the network packets before the network packets are passed to the network protocol TCP/IP (22) from the application programming interface (34). A security network driver (72) is used along with two encryption/decryption libraries (76, 90) for added data security. A network driver (40) and additional hardware (46) are also used in communication with the networks (20, 21, 50).

French Abstract

Cette invention concerne un logiciel (72) de type pilote de securite d'un reseau, lequel est insere entre le protocole de reseau TCP/IP et le pilote (40) de reseau correspondant. Des mesures de securite sont appliquees aux paquets de reseau avant que ceux-ci ne soient envoyes depuis l'interface (34) de programmation de l'application vers le protocole (22) de reseau TCP/IP. Un pilote (72) de securite du reseau est utilise en combinaison avec deux bibliotheques de cryptage/decryptage (76, 90) afin d'accroitre la securite des donnees. On utilise egalement un pilote (40) de reseau et du materiel complementaire (46) qui se trouvent en communication avec les reseaux (20, 21, 50).

Main International Patent Class: **H04L-009/00**

Fulltext Availability:

Detailed Description

Detailed Description

... 84,

After decryption, the security network driver issues (step 114, Fig, 7) a digital signature **check** call to **encapsulate** /decapsulate library 76, The swIPe **protocol header** includes a digital signature 86. The digital signature is a unique number calculated using the...

?

Claim
... sender end, a Destination address field that is assigned to the receiver end and a **Protocol field** , wherein the **tunnel** explicit multicast header comprises X bit field, a List of Addresses field, a Number of Destination field and a **Protocol** ID **field** .
16
. An apparatus for reachability **test** of explicit multicast of a receiver end, wherein the receiver end is coupled to a...
? t26/5,k/4-22,24-31,33-35

26/5,K/4 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01086242 **Image available**
REAL-TIME PACKET TRACEBACK AND ASSOCIATED PACKET MARKING STRATEGIES
TRACAGE EN TEMPS REEL DE PAQUETS ET STRATEGIES DE MARQUAGE DE PAQUETS ASSOCIEES
Patent Applicant/Assignee:
THE PENN STATE RESEARCH FOUNDATION, 304 Old Main, University Park, PA 16802-7000, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
HAMADEH Ihab, 711 University Drive, Apt # S209, State College, PA 16801, US, US (Residence), LB (Nationality), (Designated only for: US)
KESIDIS George, 692 Tanager Drive, State College, PA 16803, US, US (Residence), CA (Nationality), (Designated only for: US)
Legal Representative:
GEORGE Keith E (et al) (agent), McDermott, Will & Emery, 600 13th Street, N.W., Washington, DC 20005-3096, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200408700 A2 20040122 (WO 0408700)
Application: WO 2003US21845 20030711 (PCT/WO US03021845)
Priority Application: US 2002395838 20020712; US 2003470337 20030514
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/56
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 21592

English Abstract
To facilitate effective and efficient tracing of packet flows back to a trusted point as near as possible to the source of the flow in question, devices on the border of the trusted region are configured to mark packets with partial address information. Typically, the markings comprise fragments of IP addresses of the border devices in combination with fragment identifiers. By combining a small number of marked packets,

victims or other interested parties are able to reconstruct the IP address of each border device that forwarded a particular packet flow into the trusted region, and thereby approximately locate the source(s) of traffic without requiring the assistance of outside network operators. Moreover, traceback can be done in real-time, e.g. while a DDoS attack is on-going, so that the attack can be stopped before the victim suffers serious damage.

French Abstract

L'invention concerne des dispositifs situes sur la limite de la region fiable qui sont configures pour marquer des paquets au moyen d'informations partielles d'adresse, de maniere a faciliter et tracer de maniere efficace des flux de paquets retournant a un point fiable aussi pres que possible de la source du flux en question. Generalement, les marquages comprennent des fragments d'adresses IP des dispositifs de la limite, conjointement avec des identificateurs de fragments. La combinaison d'un petit nombre de paquets marques, de victimes ou de parties interessees permet de reconstruire l'adresse IP de chaque dispositif de la limite ayant transmis un flux de paquets specifique dans la region fiable et localisant ainsi de maniere approximativement la ou les sources de trafic, sans necessiter l'aide d'operateurs de reseau externes. De plus, le tracage peut etre effectue en temps reel, par exemple, pendant une attaque DDoS, de maniere que l'attaque puisse etre arretee avant que la victime ne presente des dommages importants.

Legal Status (Type, Date, Text)
Publication 20040122 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Detailed Description

Detailed Description

26/5,K/5 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01077196 **Image available**
METHOD AND APPARATUS FOR ENHANCED SECURITY FOR COMMUNICATION OVER A NETWORK
PROCEDE ET APPAREIL PERMETTANT D'OBTENIR UNE PLUS GRANDE SECURITE DE COMMUNICATION SUR UN RESEAU

Patent Applicant/Assignee:
NVIDIA CORPORATION, 2701 San Tomas Expressway, Santa Clara, CA 95050, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
MAUFER Thomas Albert, 20050 Rodrigues Ave., "B", Cupertino, CA 95014, US, US (Residence), US (Nationality), (Designated only for: US)
NANDA Sameer, 377 Kincora Court, San Jose, CA 95136, US, US (Residence), IN (Nationality), (Designated only for: US)
SIDENBLAD Paul J, 10190 Stonydale Drive, Cupertino, CA 95014, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
PATTERSON Todd B (agent), Moser, Patterson & Sheridan LLP, 3040 Post Oak Boulevard, Suite 1500, Houston, TX 77056, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 2003107624 A1 20031224 (WO 03107624)
Application: WO 2003US17502 20030603 (PCT/WO US0317502)
Priority Application: US 2002172352 20020613; US 2002172683 20020613; US

2002172046 20020613; US 2002172345 20020613
Parent Application/Grant:
Related by Continuation to: US 2002172352 20020613 (CIP)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
International Patent Class: H04L-029/12
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 15370
English Abstract

Method and apparatus for Internet Protocol Security (IPSec) and Network Address Translation (NAT) integration is described. Additionally, method and apparatus for enhanced security for communication over a network, and more particularly to control of security protocol negotiation to enable multiple clients to establish a virtual private network connection with a same remote address, is described. Furthermore, method and apparatus for enhanced security for communication over a network, and more particularly to NAT integration IPSec, is described. Moreover, method and apparatus for integration of NAT and source address security, including, but not limited to, determining whether a gateway computer is integrated for NAT and source address security, is described.

French Abstract

L'invention concerne un procede et un appareil d'integration de la securite du protocole internet (IPSec) et de la traduction d'adresse de reseau (NAT). L'invention concerne egalement un procede et un appareil assurant une plus grande securite de communication sur un reseau, et plus particulierement le controle de la negociation du protocole de securite pour permettre a de multiples clients d'etablir une connexion de reseau privee virtuelle avec une meme adresse eloignee. L'invention concerne, de plus, un procede et un appareil permettant d'obtenir une plus grande securite de communication sur un reseau, et plus particulierement l'integration d'IPSec a NAT. L'invention concerne en outre un procede et un appareil d'integration de NAT et de la securite d'adresse source, consistant, entre autres, a determiner si un ordinateur a passerelle est integre pour NAT et la securite d'adresse source.

Legal Status (Type, Date, Text)
Publication 20031224 A1 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... MAC address as the MAC address in the packet's MAC Source Address field, then **IPSec** packet is transmitted unchanged by the NAT gateway computer (except for decrementing the **TTL** and updating the IP **checksum** in the case of IPv4 packets; IPv6 packets are plentiful enough such that NAT is...

26/5,K/6 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01061324 **Image available**
SYSTEM, METHOD, AND PRODUCT FOR MANAGING DATA TRANSFERS IN A NETWORK
SYSTEME, PROCEDE ET PRODUIT DESTINES A GERER DES TRANSFERTS DE DONNEES DANS UN RESEAU

Patent Applicant/Assignee:
INTERNATIONAL BUSINESS MACHINES CORPORATION, New Orchard Road, Armonk, NY 10504, US, US (Residence), US (Nationality)
IBM UNITED KINGDOM LIMITED, PO Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU, GB, GB (Residence), GB (Nationality), (Designated only for: MG)
Inventor(s):
BEUKEMA Bruce Leroy, 71050 210th Avenue, Hayfield, MN 55940, US,
GREGG Thomas Anthony, 121 Bellevue Road, Highland, NY 12528, US,
NEAL Danny Marvin, 4604 Hightower Drive, Round Rock, TX 78681, US,
RECIO Renato John, 6707 Winnepeg Cove, Austin, TX 78759, US,
Legal Representative:
BURT Roger James (agent), IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN, GB,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200391888 A2-A3 20031106 (WO 0391888)
Application: WO 2003GB1416 20030401 (PCT/WO GB03001416)
Priority Application: US 2002132456 20020425
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-013/42
International Patent Class: G06F-013/40; H04L-029/06; H04L-029/08; **G06F-015/17** ; G06F-013/12
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10953

English Abstract
A method, system, and product in a data processing system for managing data transmitted from a first end node to a second end node included in the data processing system. A logical connection is established between the first end node and the second end node prior to transmitting data between the end nodes. An instance number is associated with the logical connection and included in each packet transmitted between end nodes while this connection remains. The number remains constant during this connection, but is altered, such as by incrementing it, each time a logical connection between these end nodes is reestablished. Each packet is associated with a particular instance of the logical connection and when it is received, the number may be used to determine whether the packet is a stale packet transmitted during a previous logical connection between these end nodes.

French Abstract
L'invention concerne un procede, un systeme et un produit permettant de gerer, dans un systeme de traitement de donnees, des donnees transmises a partir d'un premier noeud d'extremite compris dans ce systeme de traitement de donnees. Une connexion logique est etablie entre le premier noeud d'extremite et le second noeud d'extremite avant la transmission des donnees entre les noeuds d'extremite. Un numero d'instance est associe a la connexion logique et inclus dans chaque paquet transmis entre les noeuds d'extremite tant que la connexion est etablie. Le numero reste constant pendant cette connexion, mais est modifie, notamment par incrementation, a chaque fois qu'une connexion logique entre ces noeuds d'extremite est reetablie. Chaque paquet est associe a une instance particuliere de la connexion logique, et, lorsqu'il est recu, le numero peut etre utilise pour determiner si le paquet est un paquet perime transmis pendant une connexion logique precedente entre lesdits noeuds d'extremite.

Legal Status (Type, Date, Text)
Publication 20031106 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20040304 Late publication of international search report
Republication 20040304 A3 With international search report.
Republication 20040304 A3 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

...International Patent Class: **G06F-015/17**
Fulltext Availability:
Detailed Description

Detailed Description

26/5,K/7 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01060071 **Image available**
METHOD TO PROVIDE DYNAMIC INTERNET PROTOCOL SECURITY POLICY SERVICES
PROCEDE DESTINE A FOURNIR DES SERVICES DYNAMIQUES EN MATIERE DE REGLES DE PROTOCOLE DE SECURITE INTERNET
Patent Applicant/Assignee:
3COM CORPORATION, 5500 Great America Boulevard, Santa Clara, CA 95052, US , US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
AMARA Satish, 1833 West Golf Road, #168, Mount Prospect, IL 60056, US, US (Residence), IN (Nationality), (Designated only for: US)
VERMA Madhvi, 1300 East Algonquin Road, #2N, Schaumburg, IL 60073, US, US (Residence), IN (Nationality), (Designated only for: US)
Legal Representative:
HARRIS Brian R (agent), McDonnell Boehnen Hulbert & Berghoff, 300 South Wacker Drive, Chicago, IL 60606, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200390041 A2 20031030 (WO 0390041)
Application: WO 2003US8800 20030319 (PCT/WO US0308800)
Priority Application: US 2002101641 20020320
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW

Patent and Priority Information (Country, Number, Date):
  Patent: WO 200412394 A1 20040205 (WO 0412394)
  Application: WO 2002KR1448 20020731 (PCT/WO KR02001448)
  Priority Application: WO 2002KR1448 20020731
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU
  CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
  KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU
  SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
  (EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
  (OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
  (AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
  (EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/26
Publication Language: English
Filing Language: Korean
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 4012

English Abstract
  The present invention relates to method and apparatus for receivability test and reachability test of explicit multicast packet. The xcast receivability test according to the present invention comprises the steps of: at a sender end, sending a receivability probe packet to a receiver end; at the receiver end, receiving the receivability probe packet; generating an ICMP error message-Destination Unreachable; sending the ICMP error message-Destination Unreachable to sender end; at the sender end, receiving the ICMP error message-Destination Unreachable; and analyzing the ICMP error message-Destination Unreachable.

French Abstract
  L'invention concerne un procede et un appareil destines a des tests de recevabilite et a des tests d'accessibilite de paquets multidestination explicite. Le test de recevabilite multidestination selon l'invention comprend les etapes suivantes : a un terminal emetteur, envoi d'un paquet test de recevabilite a un terminal recepteur ; au terminal recepteur, reception du paquet test de recevabilite ; generer un message d'erreur ICMP destination inaccessible ; emission du message d'erreur ICPM destination inaccessible au terminal emetteur ; au terminal emetteur, reception dudit message d'erreur ; et analyse du message d'erreur ICPM destination inaccessible.

Legal Status (Type, Date, Text)
Publication 20040205 A1 With international search report.

Fulltext Availability:
  Detailed Description
  Claims

Detailed Description
... address, which is specially assigned for xcast, as a
  7
  destination address. Also, because TFL(**Time** -to- **Live**) value in the **tunnel** IP header of the reachability probe packet P 500 is set in proportion to the number of generation of probe packet, the validity of **TTL** value is **checked** every time the probe packetpasses through each router, transit node.

  FIGA shows the first step of xcast reachability **test** . In the **test** , because the TTL value is set to 1 and the destination of IP header is...

File 348:EUROPEAN PATENTS 1978-2004/Mar W01
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040311,UT=20040304
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	8612	TTL OR TTF OR TIME(1W)(LIVE OR LIFE)
S2	699	(HOP OR HOPS)(2N)(LIMIT??? ? OR LIMITATION? OR COUNT??? ? - OR ALLOW?)
S3	3597	(IP OR INTERNET OR PROTOCOL OR ICMP OR DNS)(1W)(FIELD? ? OR HEADER? ?)
S4	31022	TUNNEL???? ? OR TRANSPORT??? ?(1W)(MODE OR MODES)
S5	1334	IPSEC OR IP()SECURITY OR L2TP OR PPTP OR SOCKSV5 OR SOCKS(-)V5 OR LAYER()(TWO OR 2)()FORWARD??? ? OR L2F
S6	3484	VPN OR VPNS OR VIRTUAL()PRIVATE()(NET OR NETWORK? ?)
S7	285341	ENCAPSULAT? OR WRAP???? ? OR INSULAT?
S8	18882	(SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHER?)(2N)(CONNECT???? ? OR CONNECTIVIT? OR CHANNEL? ? OR PATH? ? OR PATHWAY? OR PASSAGE? ?)
S9	13539	(SECURE? ? OR SECURITY OR ENCRYPT? OR ENCIPHER? OR ENCYPHER?)(2N)(COMMUNICAT???? ? OR ACCESS OR ACCESS?? ? OR ACCESSING)
S10	7651	PRIVATE(1W)(NET OR NETS OR NETWORK?)
S11	1782076	VERIFY? OR VERIFIE? ? OR VERIFICATION? OR VALIDAT? OR CHECK??? ? OR CHEQU? OR EXAMIN? OR TEST OR TESTS OR TESTED OR TESTING? OR EVALUAT? OR CONFIRM?
S12	25790	AUTHENTICAT? OR SUBSTANTIAT? OR RECHECK? OR RECHEQ? OR CROSSCHECK? OR CROSSCHEQ? OR DOUBLECHECK? OR DOUBLECHEQU?
S13	704	S1:S3(25N)S4:S10
S14	142	S13(25N)S11:S12
S15	12	S14/TI,AB,CM
S16	6110	IC='H04L-009'
S17	15382	IC='G06F-015'
S18	28	S14 AND S16:S17
S19	16905	S4:S10(15N)S11:S12
S20	102	S14(25N)S19
S21	114	S1:S2(25N)S4:S10
S22	21	S21(25N)S11:S12
S23	54	S15 OR S18 OR S22
S24	54	IDPAT (sorted in duplicate/non-duplicate order)
S25	53	IDPAT (primary/non-duplicate records only)
S26	35	S25 NOT (WIND()TUNNEL? OR TUNNEL()BAT OR LOGIC OR TRANSISTOR? OR DIODE?)

26/5,K/3 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01089554 **Image available**
METHOD AND APPARATUS FOR RECEIVABILITY TEST AND REACHABILITY TEST OF EXPLICIT MULTICAST
PROCEDE ET APPAREIL DE TEST DE RECEVABILITE ET DE TEST D'ACCESSIBILITE MULTIDESTINATION EXPLICITE
Patent Applicant/Assignee:
KTFREETEL CO LTD, 890-20 Daechi-dong, Gangnam-gu, 135-280 Seoul, KR, KR (Residence), KR (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
LEE Ji-Woong, #501 1357-63 Seocho-dong, Seocho-gu, 137-070 Seoul, KR, KR (Residence), KR (Nationality), (Designated only for: US)
Legal Representative:
LEE Kyeong-Ran (agent), 502 BYC Bldg., 648-1 Yeoksam 1-dong, Kangnam-ku, 135-081 Seoul, KR,